

Beetle

Sharing, flexibility and access control for Bluetooth Low Energy

Amit Levy James Hong Laurynas Riliskis
Philip Levis Keith Winstein

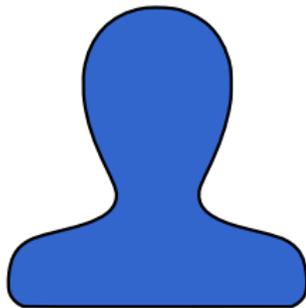
Stanford University

June 24, 2016

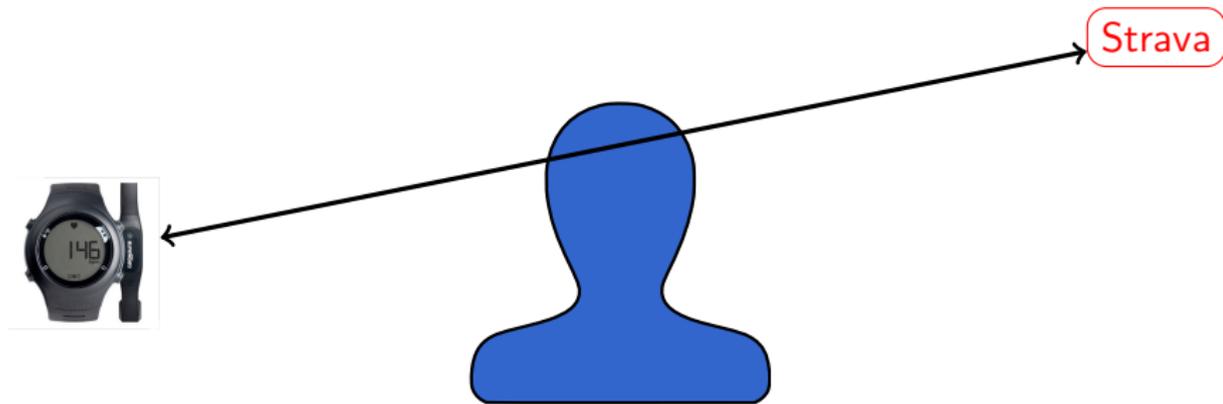
Meet Grace



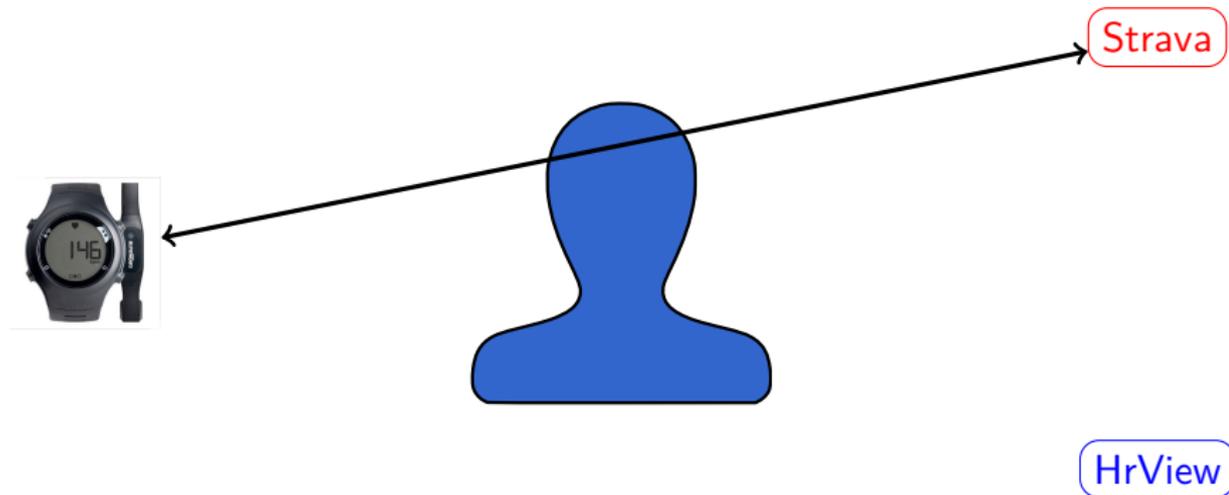
Meet Grace



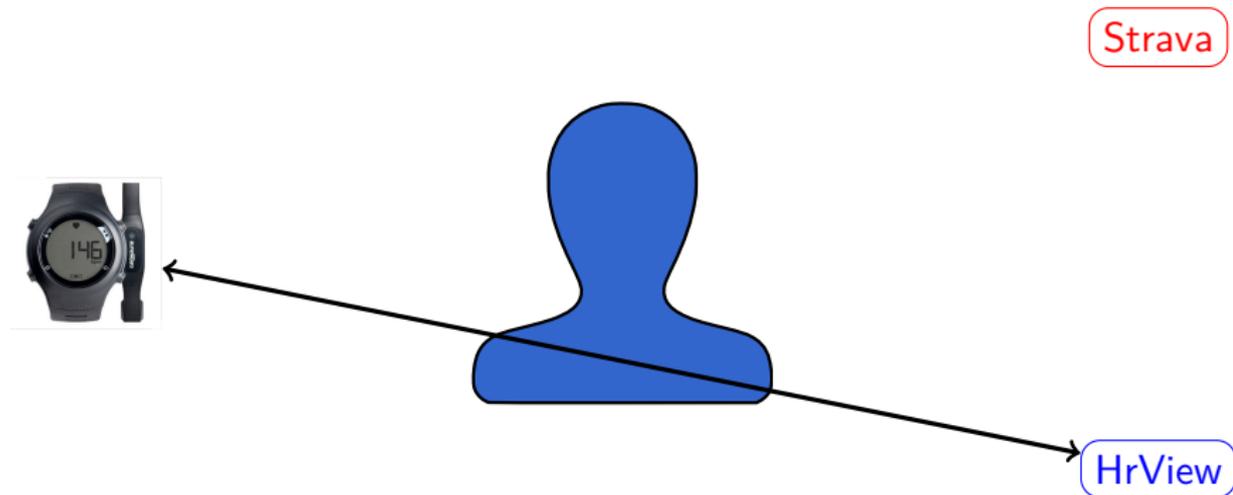
Meet Grace



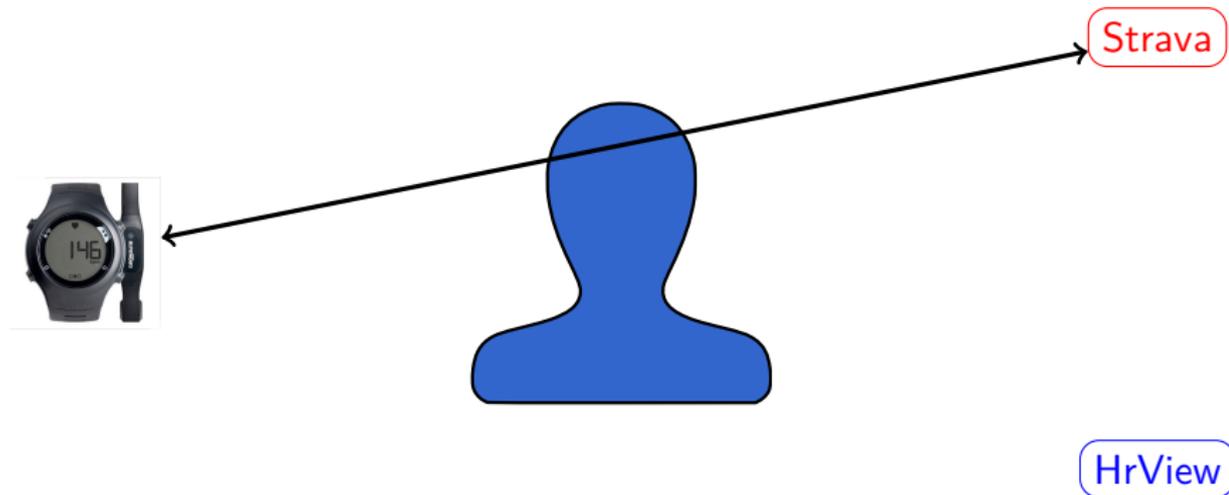
Meet Grace



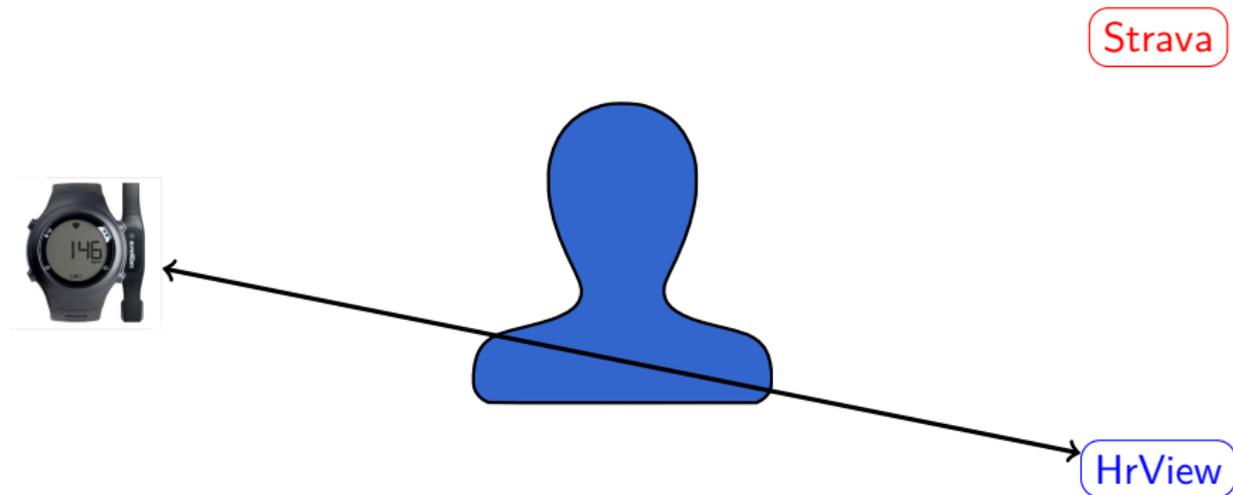
Meet Grace



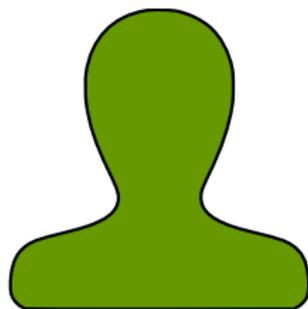
Meet Grace



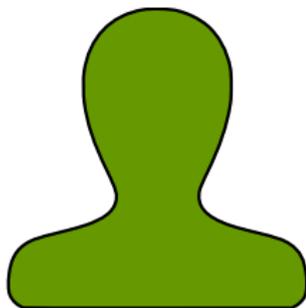
Meet Grace



Meet Fabian



Meet Fabian

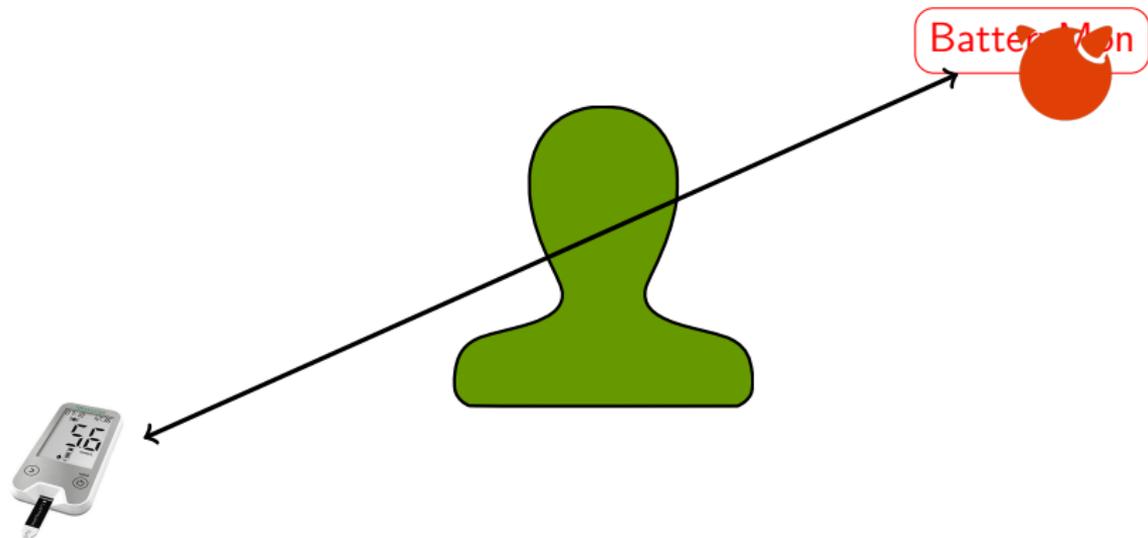


Meet Fabian

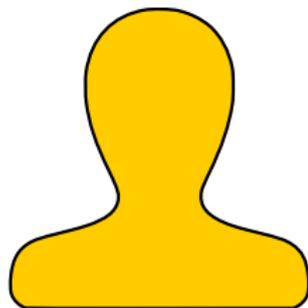
BatteryMon



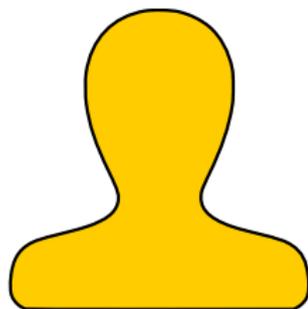
Meet Fabian



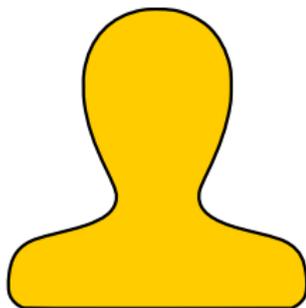
Meet Esther



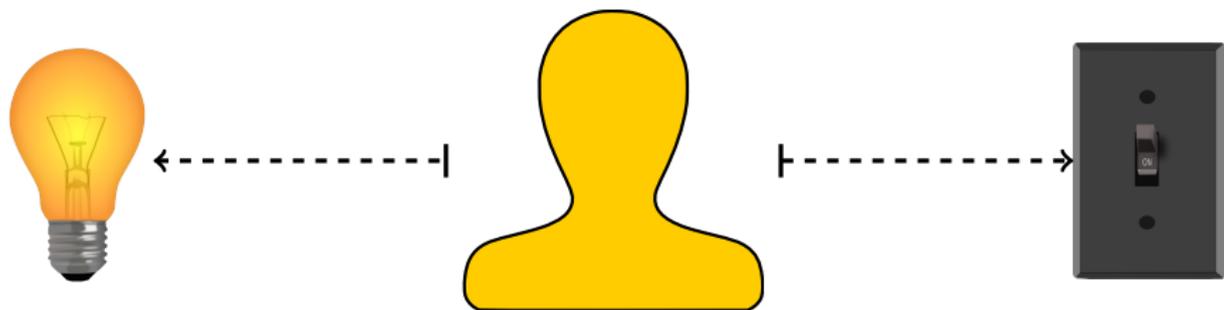
Meet Esther

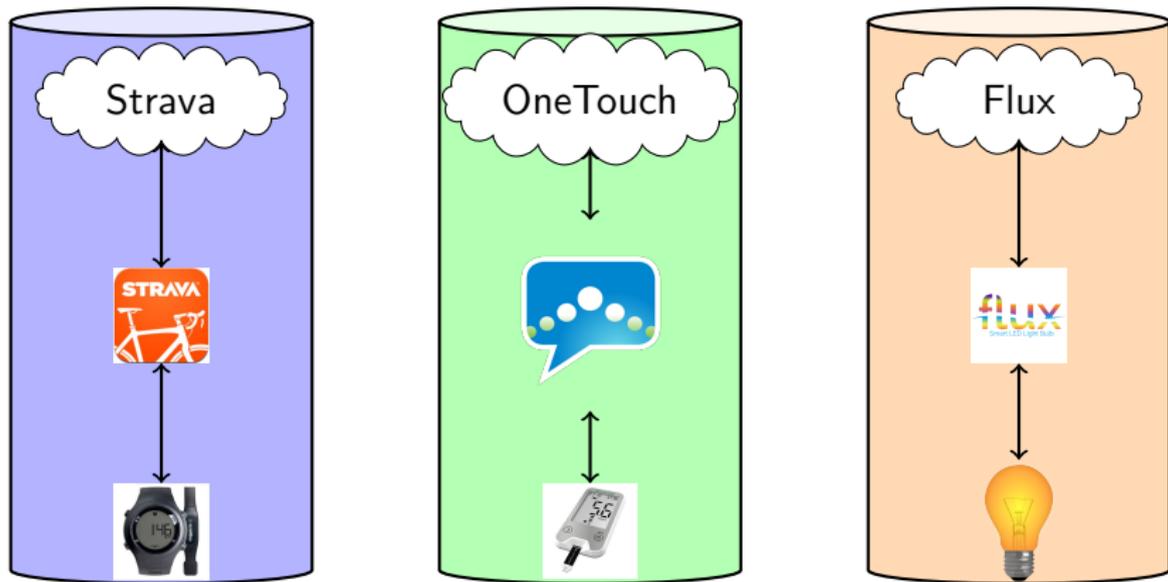


Meet Esther



Meet Esther





No extensibility, no access control, limited communication

Limitations of Bluetooth Low Energy (BLE)

1. Applications must run on the gateway
2. One application at a time
3. All-or-nothing access

Peripherals need to be simple

- ▶ Low cost
- ▶ Low power
- ▶ Hard to update

Gateway oblivious to peripheral functionality

- ▶ How to virtualize generally?
- ▶ Who can access what?

The gateway should enable
flexible and safe sharing

Sharing

Applications can safely share access to peripherals without explicit coordination.

Access Control

Users can specify fine-grained access policies on peripherals and applications.

Communication flexibility

Many-to-many communication between peripherals, gateway applications and cloud applications.

Backwards compatible

Doesn't require changes to existing peripherals or applications.

Current Gateways: Explicit support

Dedicated drivers understand a class of peripherals:

- ▶ Printers
- ▶ Keyboards
- ▶ Disks

Current Gateways: Explicit support

Dedicated drivers understand a class of peripherals:

- ▶ Printers
- ▶ Keyboards
- ▶ Disks

Pros

- ▶ Safe virtualization
- ▶ Access control

Cons

- ▶ Need a trusted module for each device class
- ▶ Has worked OK for desktops, but does it scale?

Current Gateways: Exclusive access from one application

For special case peripherals, gateway provides an exclusive, raw channel:

- ▶ Oscilloscope, hardware debugger
- ▶ USB breathalyzer, USB blood pressure monitor
- ▶ Most IoT peripherals (door locks, lights, fitness bands)

Current Gateways: Exclusive access from one application

For special case peripherals, gateway provides an exclusive, raw channel:

- ▶ Oscilloscope, hardware debugger
- ▶ USB breathalyzer, USB blood pressure monitor
- ▶ Most IoT peripherals (door locks, lights, fitness bands)

Pros

- ▶ Don't need explicit support for each new device class

Cons

- ▶ Can't allow multiple apps to use peripheral
- ▶ App gets complete control over peripheral

Current Gateway Systems

OS	Explicit Driver	Exclusive Access
HomeOS	✓	
Linux	✓	✓ (BLE sockets)
Android	✓ (Google Health)	✓
iOS	✓ (Health/HomeKit)	✓

Explicit support

Impractical for operating systems to anticipate new device functionality

vs.

Exclusive access

No sharing, no access control, inflexible communication

Bluetooth Low Energy application protocol

Bluetooth Low Energy application protocol

Attribute Protocol (ATT):

- ▶ Key-type-value store
- ▶ Transactional flow-control
- ▶ READ, WRITE, NOTIFY,
FIND-BY-TYPE...

Bluetooth Low Energy application protocol

Attribute Protocol (ATT):

- ▶ Key-type-value store
- ▶ Transactional flow-control
- ▶ READ, WRITE, NOTIFY, FIND-BY-TYPE...

Generic Attribute Profile (GATT):

- ▶ Structure over attributes
- ▶ Characteristic: Groups attributes for a value
- ▶ Services: Groups related characteristics

Bluetooth Low Energy application protocol

Attribute Protocol (ATT):

- ▶ Key-type-value store
- ▶ Transactional flow-control
- ▶ READ, WRITE, NOTIFY, FIND-BY-TYPE...

Generic Attribute Profile (GATT):

- ▶ Structure over attributes
- ▶ Characteristic: Groups attributes for a value
- ▶ Services: Groups related characteristics

Example, heart rate monitor



Bluetooth Low Energy application protocol

Attribute Protocol (ATT):

- ▶ Key-type-value store
- ▶ Transactional flow-control
- ▶ READ, WRITE, NOTIFY, FIND-BY-TYPE...

Generic Attribute Profile (GATT):

- ▶ Structure over attributes
- ▶ Characteristic: Groups attributes for a value
- ▶ Services: Groups related characteristics

Example, heart rate monitor

Find Char with UUID HRM



Bluetooth Low Energy application protocol

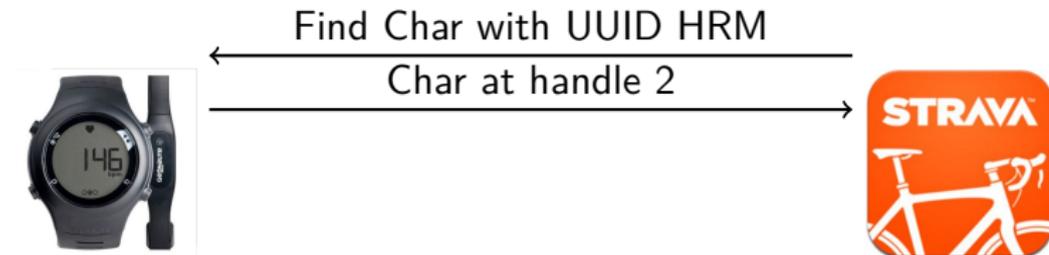
Attribute Protocol (ATT):

- ▶ Key-type-value store
- ▶ Transactional flow-control
- ▶ READ, WRITE, NOTIFY, FIND-BY-TYPE...

Generic Attribute Profile (GATT):

- ▶ Structure over attributes
- ▶ Characteristic: Groups attributes for a value
- ▶ Services: Groups related characteristics

Example, heart rate monitor



Bluetooth Low Energy application protocol

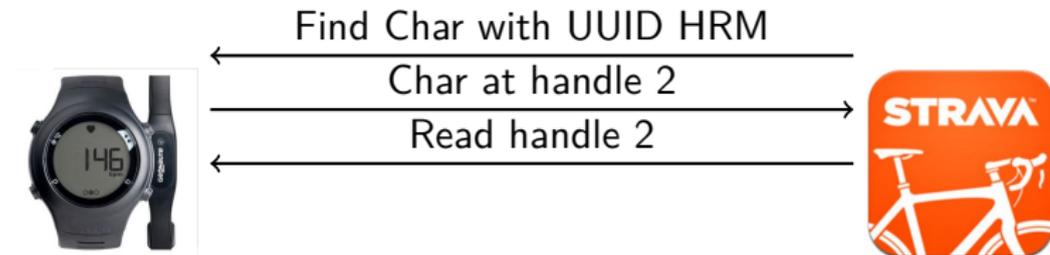
Attribute Protocol (ATT):

- ▶ Key-type-value store
- ▶ Transactional flow-control
- ▶ READ, WRITE, NOTIFY, FIND-BY-TYPE...

Generic Attribute Profile (GATT):

- ▶ Structure over attributes
- ▶ Characteristic: Groups attributes for a value
- ▶ Services: Groups related characteristics

Example, heart rate monitor



Bluetooth Low Energy application protocol

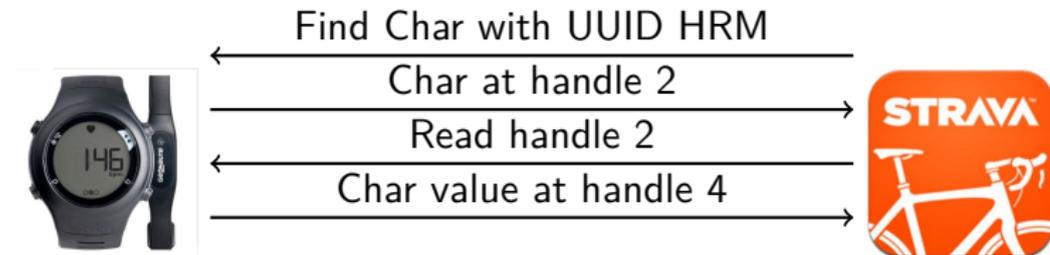
Attribute Protocol (ATT):

- ▶ Key-type-value store
- ▶ Transactional flow-control
- ▶ READ, WRITE, NOTIFY, FIND-BY-TYPE...

Generic Attribute Profile (GATT):

- ▶ Structure over attributes
- ▶ Characteristic: Groups attributes for a value
- ▶ Services: Groups related characteristics

Example, heart rate monitor



Bluetooth Low Energy application protocol

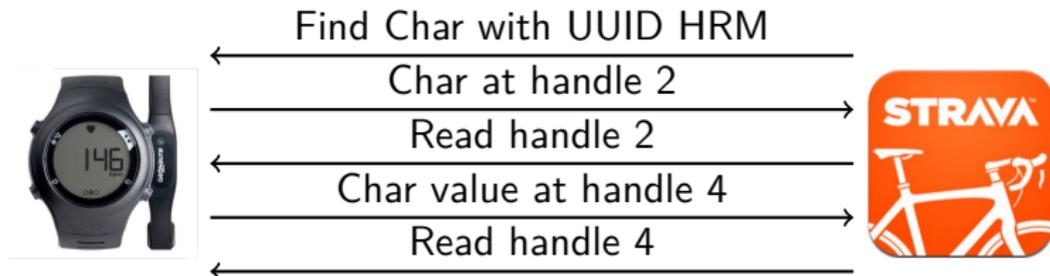
Attribute Protocol (ATT):

- ▶ Key-type-value store
- ▶ Transactional flow-control
- ▶ READ, WRITE, NOTIFY, FIND-BY-TYPE...

Generic Attribute Profile (GATT):

- ▶ Structure over attributes
- ▶ Characteristic: Groups attributes for a value
- ▶ Services: Groups related characteristics

Example, heart rate monitor



Bluetooth Low Energy application protocol

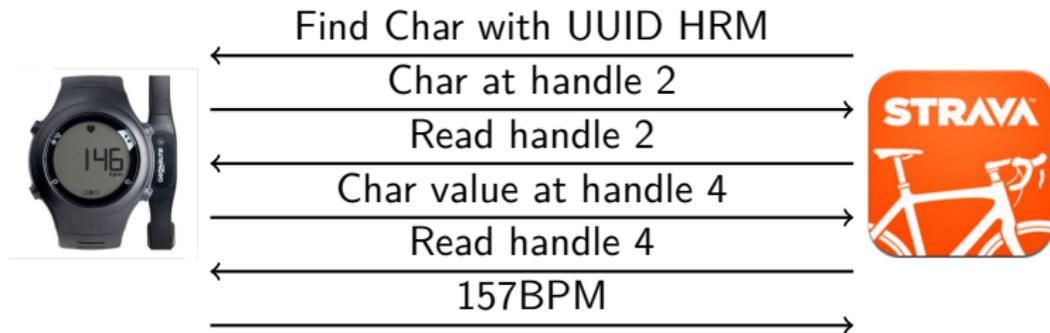
Attribute Protocol (ATT):

- ▶ Key-type-value store
- ▶ Transactional flow-control
- ▶ READ, WRITE, NOTIFY, FIND-BY-TYPE...

Generic Attribute Profile (GATT):

- ▶ Structure over attributes
- ▶ Characteristic: Groups attributes for a value
- ▶ Services: Groups related characteristics

Example, heart rate monitor

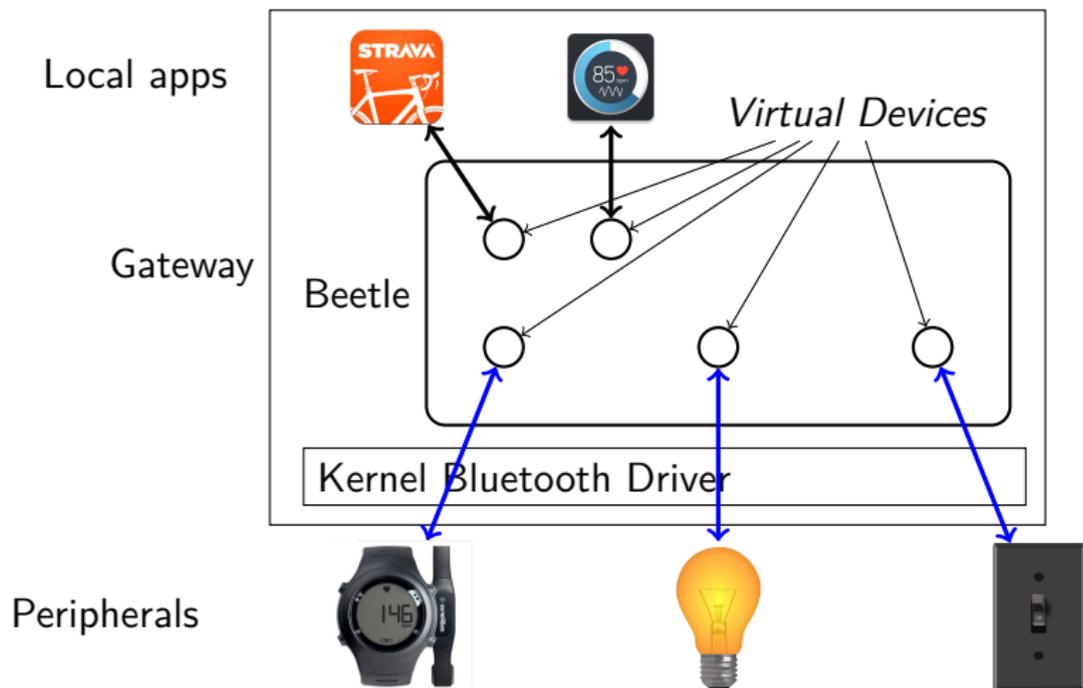


Beetle: Key insight

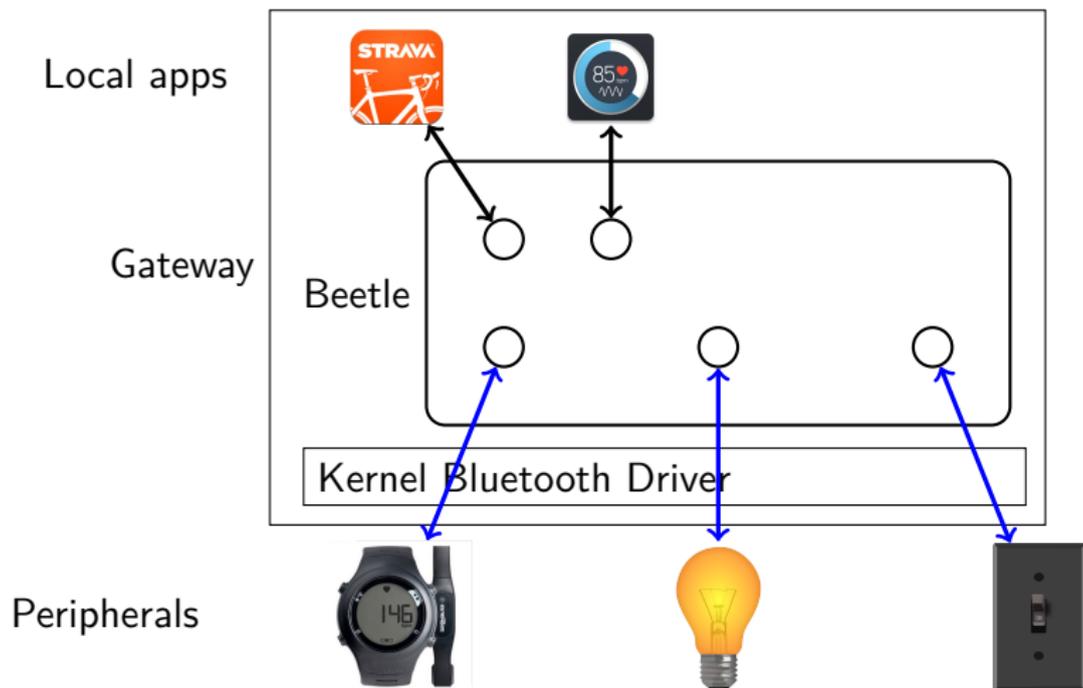
BLE application protocol (GATT) is amenable to multiplexing:

- ▶ Unified data model
- ▶ Standardized data types
- ▶ Transactions are meaningful to applications

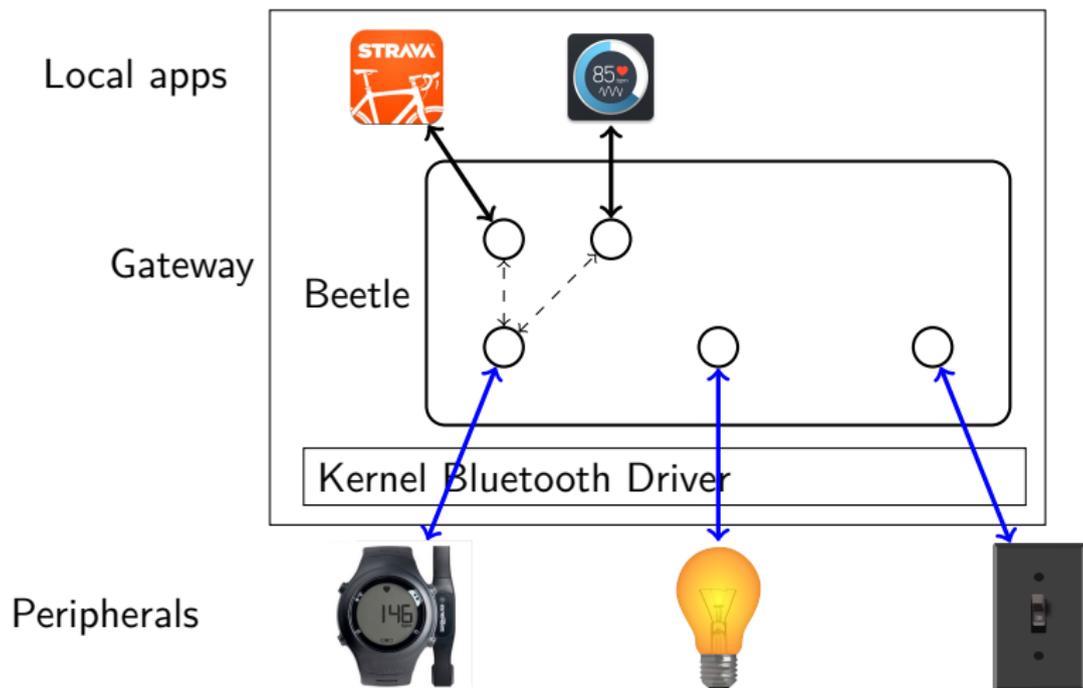
Beetle Architecture



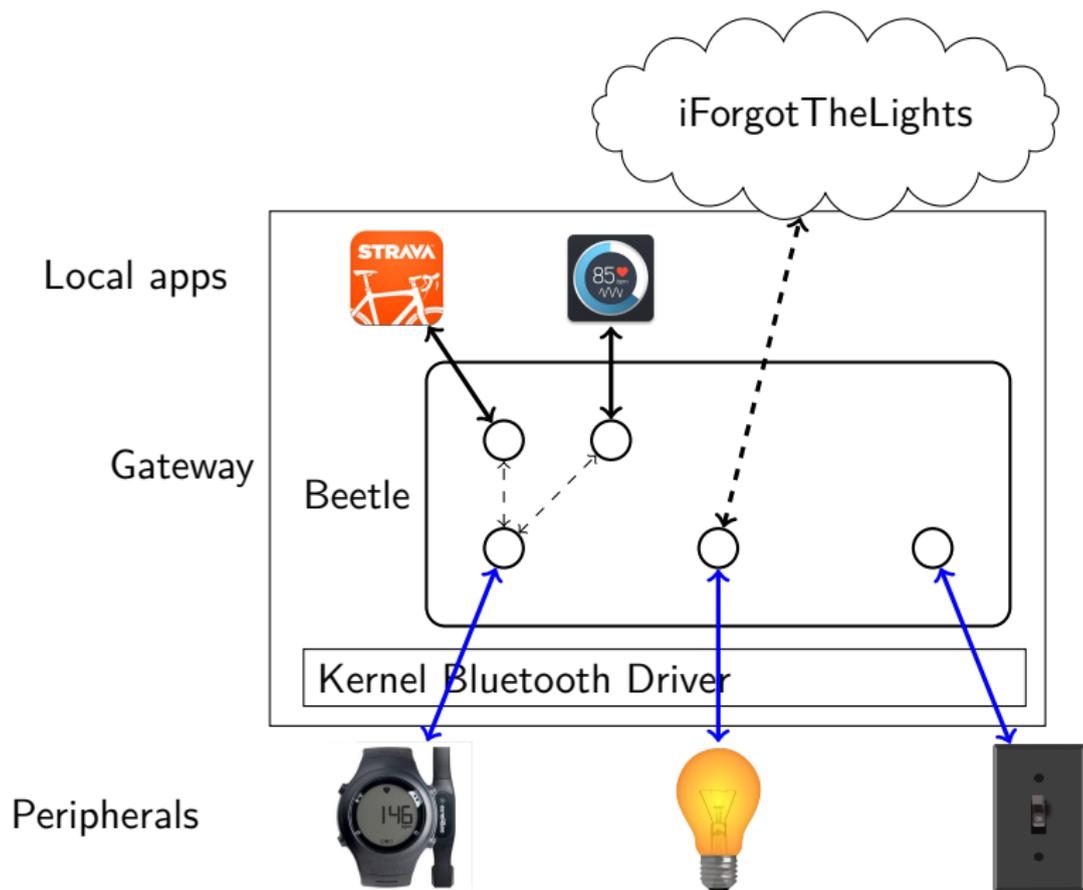
Beetle Architecture



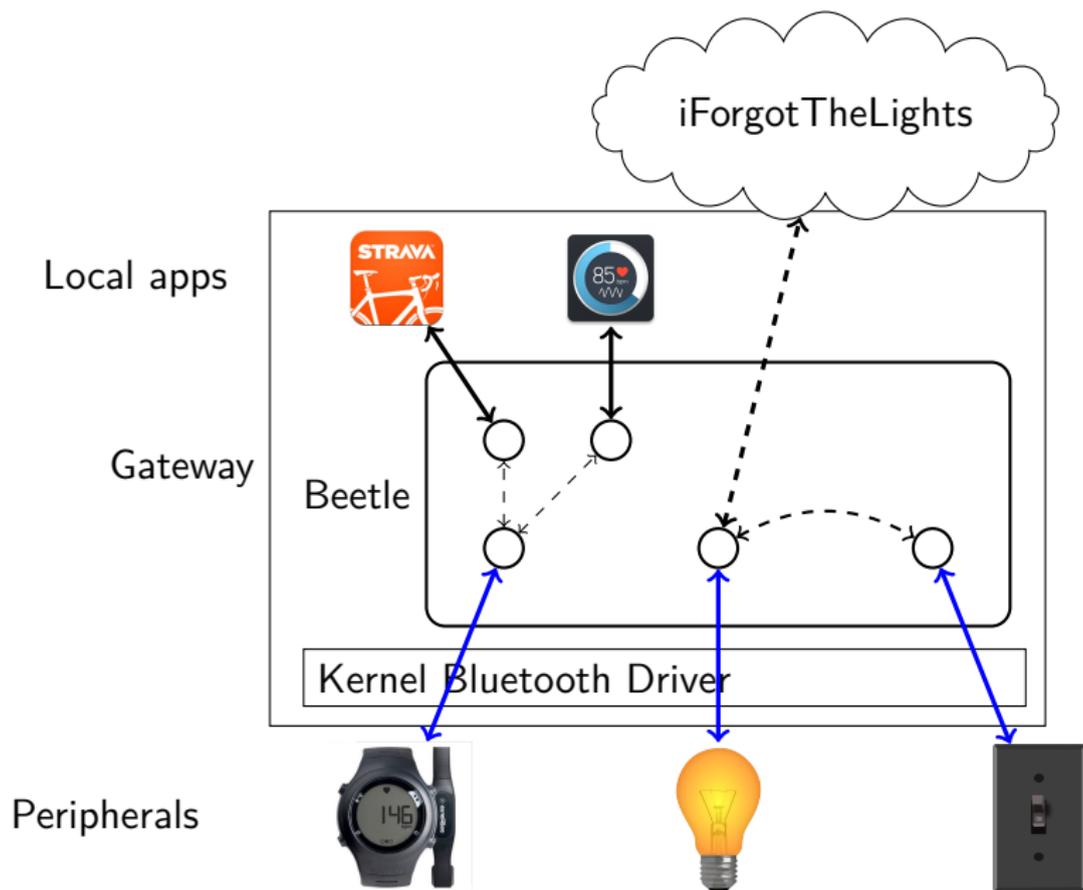
Beetle Architecture



Beetle Architecture



Beetle Architecture



Virtual Devices: Just speak GATT

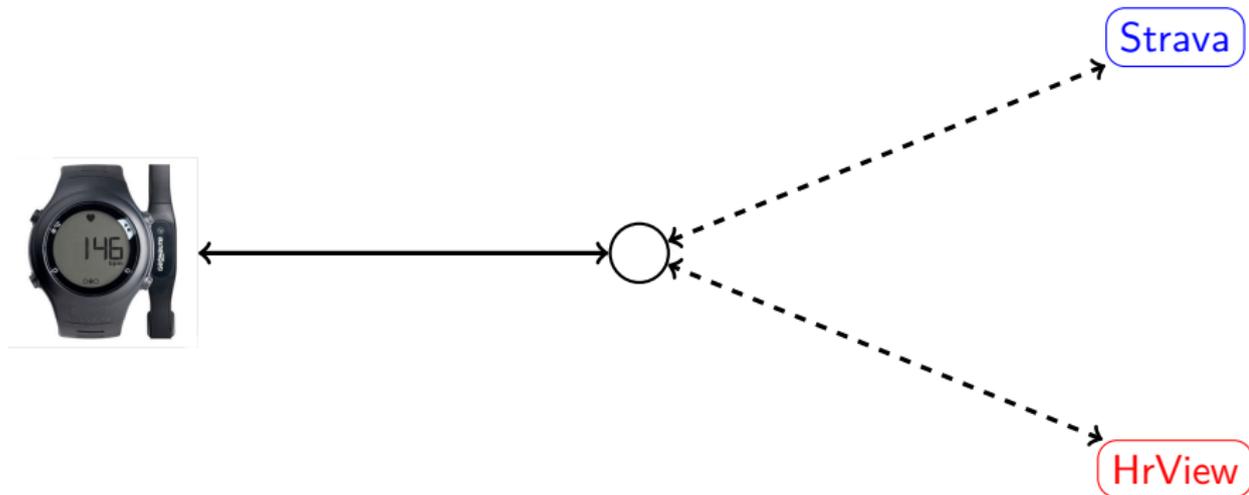
Look like a peripheral to applications.

Look like a gateway to peripherals.

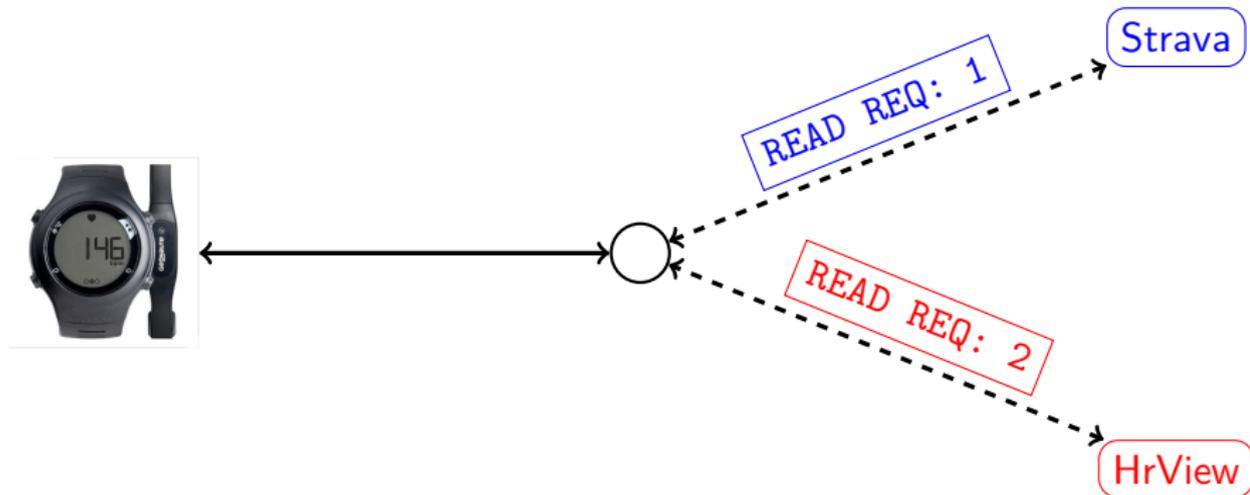
Provide:

- ▶ Sharing by multiplexing transactions from different clients
- ▶ Access control by mapping handle space
- ▶ Flexible communication by allowing transactions over any link

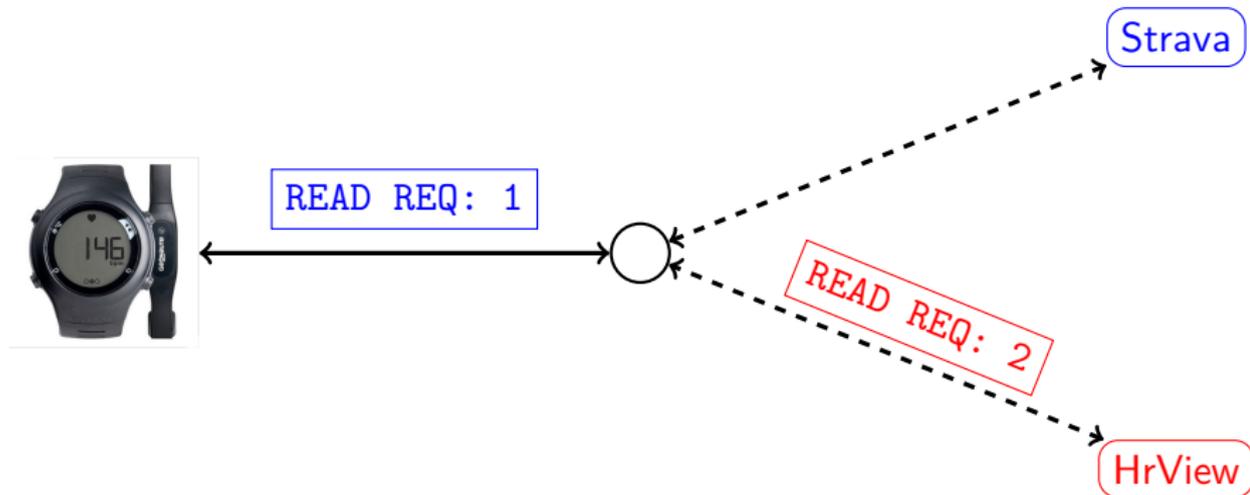
Virtual Devices: Sharing



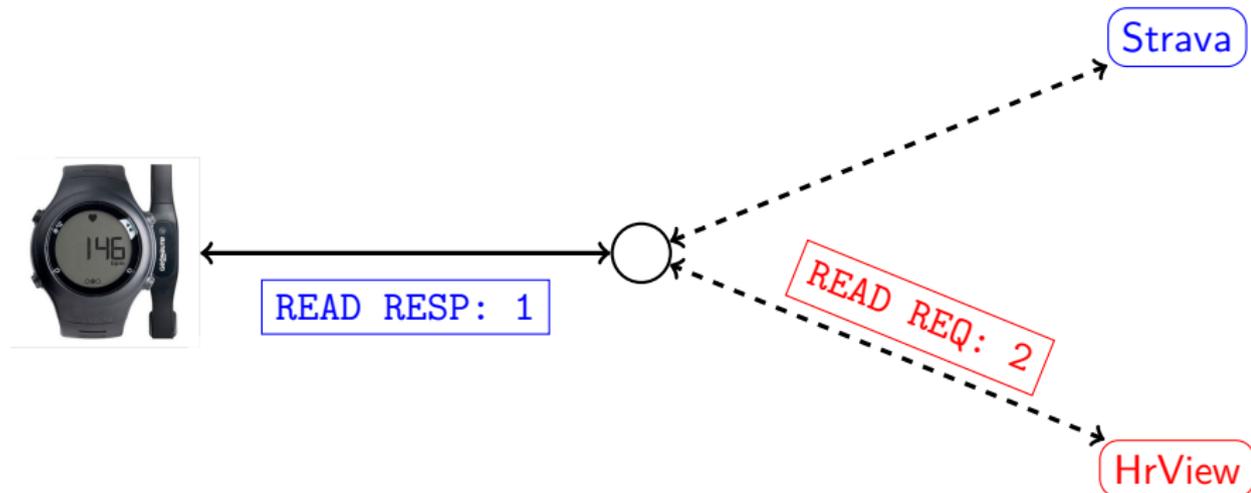
Virtual Devices: Sharing



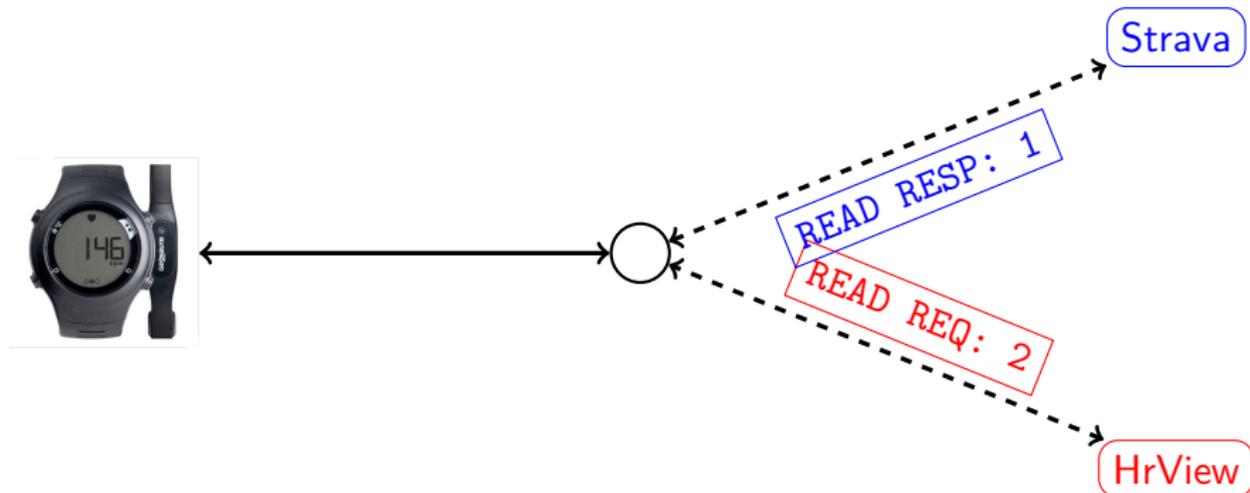
Virtual Devices: Sharing



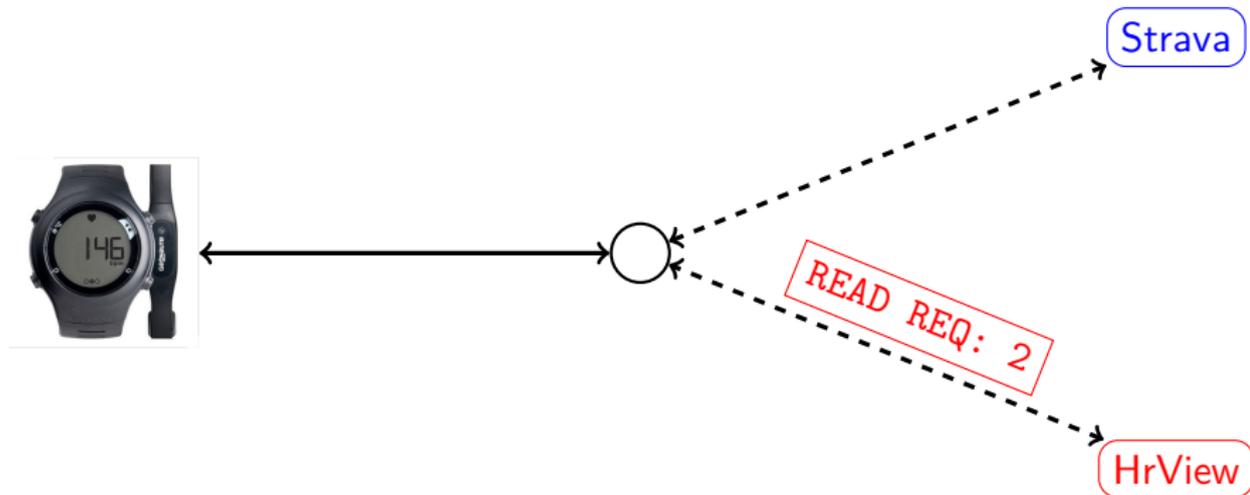
Virtual Devices: Sharing



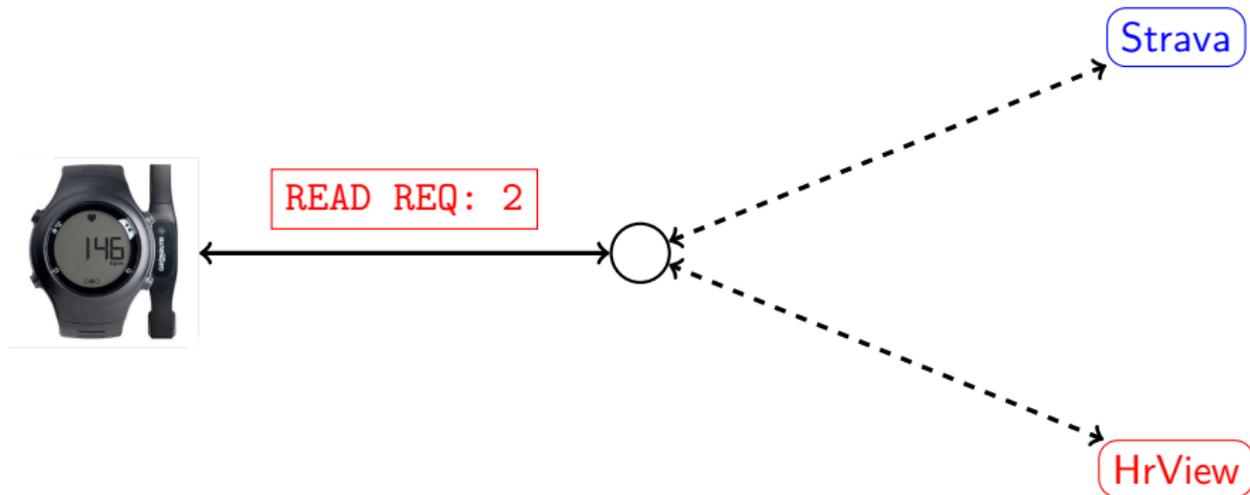
Virtual Devices: Sharing



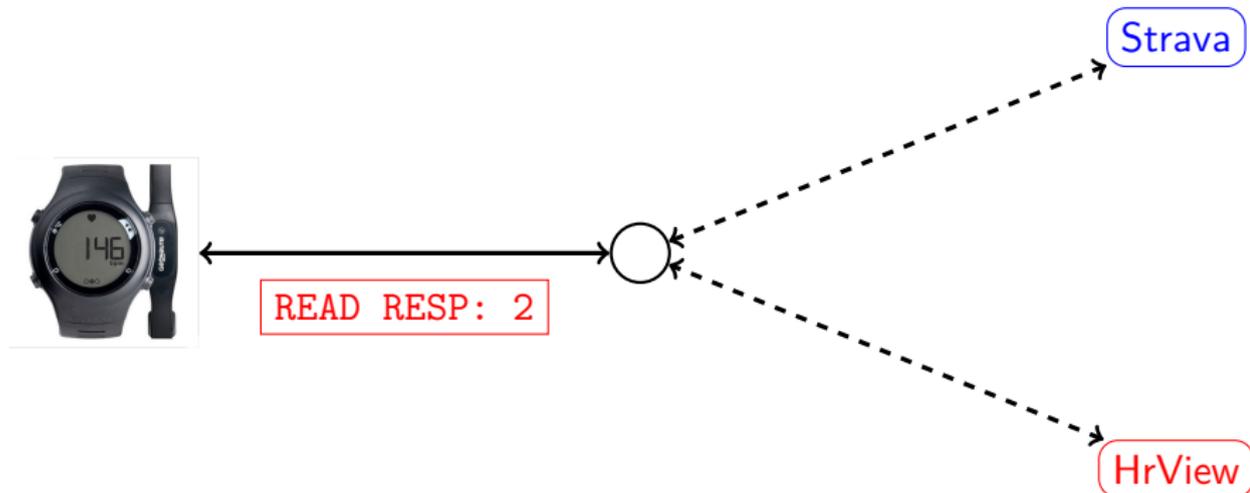
Virtual Devices: Sharing



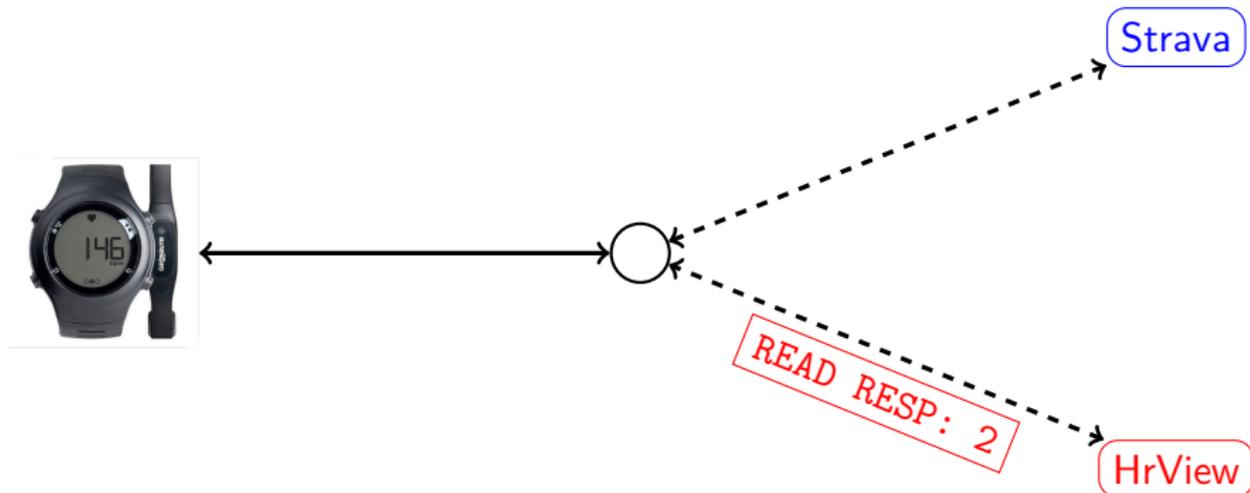
Virtual Devices: Sharing



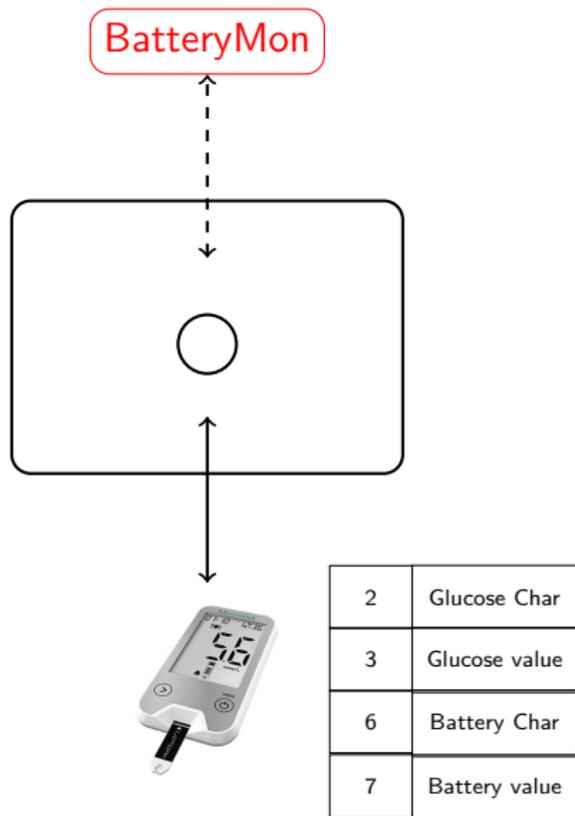
Virtual Devices: Sharing



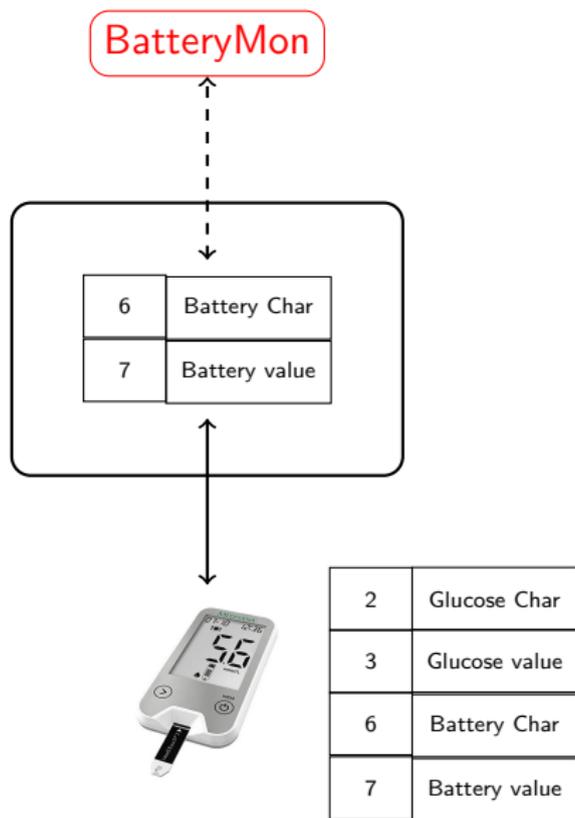
Virtual Devices: Sharing



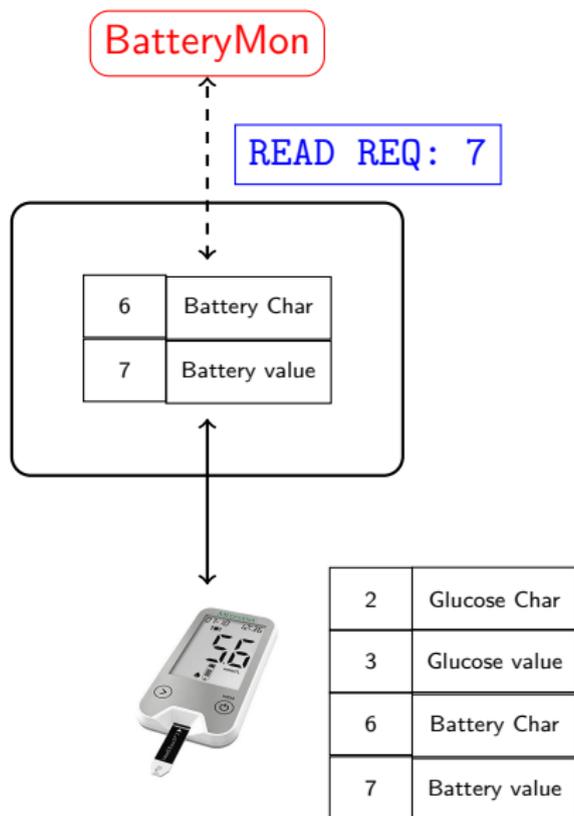
Virtual Devices: Access Control



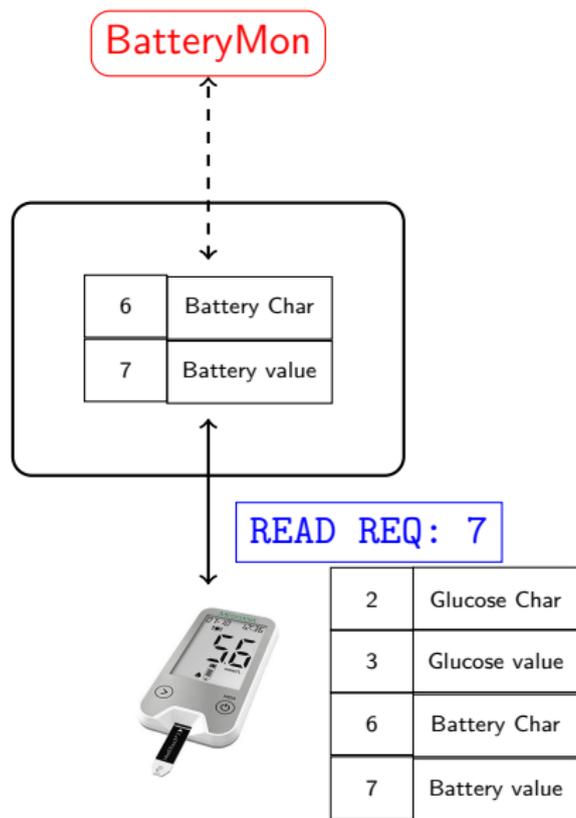
Virtual Devices: Access Control



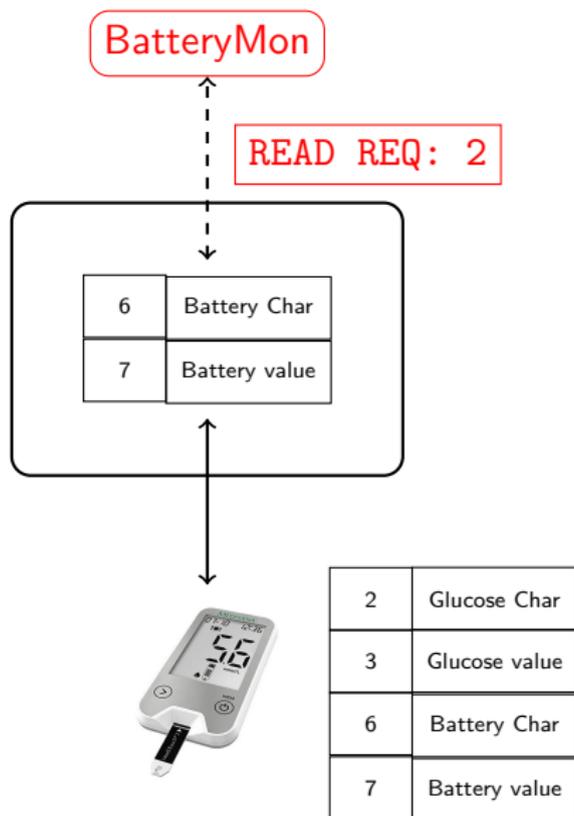
Virtual Devices: Access Control



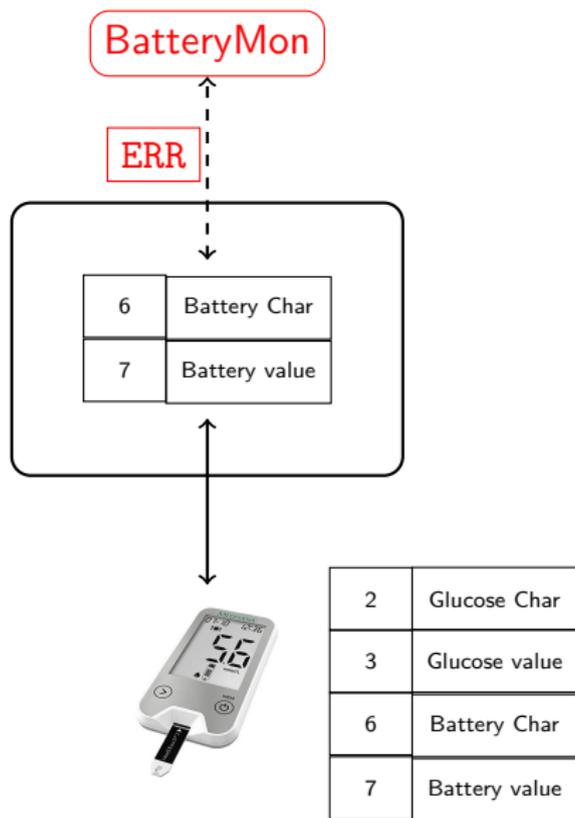
Virtual Devices: Access Control



Virtual Devices: Access Control



Virtual Devices: Access Control



Implementation

Linux

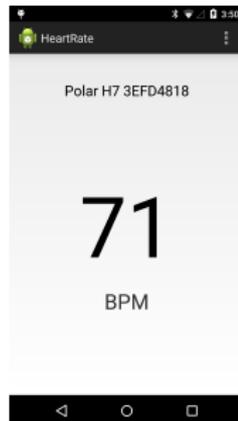
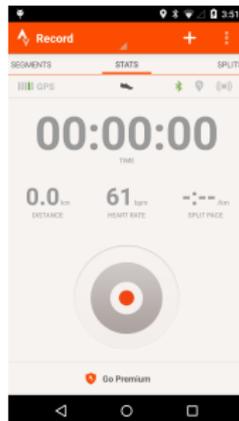
- ▶ User-space daemon (C++)
- ▶ Applications connect via UNIX domain or TCP sockets
- ▶ Access control via database + browser interface

Android

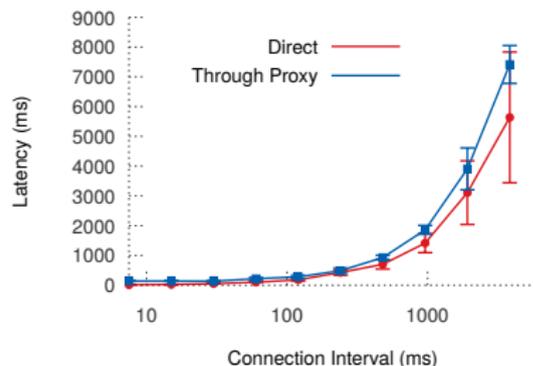
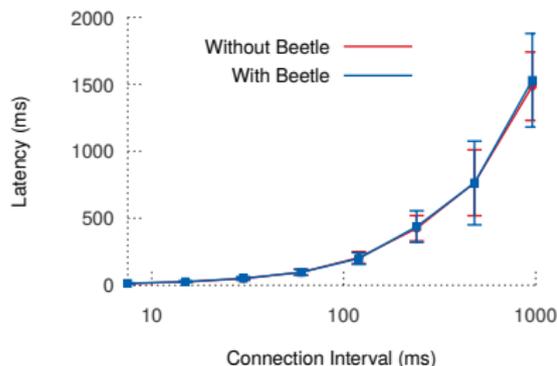
- ▶ Modified Android's Bluetooth Service app
- ▶ Applications connect over Intents (IPC)
- ▶ Access control via normal user control flow

Applications

- ▶ Multi-app Heart Rate Monitor
- ▶ Battery Monitor
- ▶ Generic Home Gateway



Performance



- ▶ One app to one peripheral – no significant overhead
 - ▶ 1.7x connection interval with/without Beetle
- ▶ Multi-client throughput depends on workload
 - ▶ Reads are linearly scalable via caching
- ▶ Peripheral-to-peripheral $\sim 2\text{-}3\text{x}$ due to extra hop
 - ▶ Could be improved with better coordination by gateway

Limitations

- ▶ Bluetooth Low Energy specific
 - ▶ Relies on properties of the application layer protocol
- ▶ Peripherals must conform to GATT transactional semantics
 - ▶ But peripheral-specific virtual devices could mask violations
- ▶ Access control does not solve secure naming
- ▶ Does not offer a management solution
 - ▶ Complimentary to systems, like HomeOS

Discussion

Safe and flexible peripheral sharing

Can and should be provided first-class by the gateway

Discussion

Safe and flexible peripheral sharing

Can and should be provided first-class by the gateway

Lessons for protocol design

- ▶ Data model at the right abstraction level
- ▶ Standardized data types
- ▶ Global namespace

Discussion

Safe and flexible peripheral sharing

Can and should be provided first-class by the gateway

Lessons for protocol design

- ▶ Data model at the right abstraction level
- ▶ Standardized data types
- ▶ Global namespace

Lessons for BLE peripheral builders

- ▶ Don't rely on exclusive access for semantics
- ▶ One GATT transaction per application transaction

Discussion

Safe and flexible peripheral sharing

Can and should be provided first-class by the gateway

Lessons for protocol design

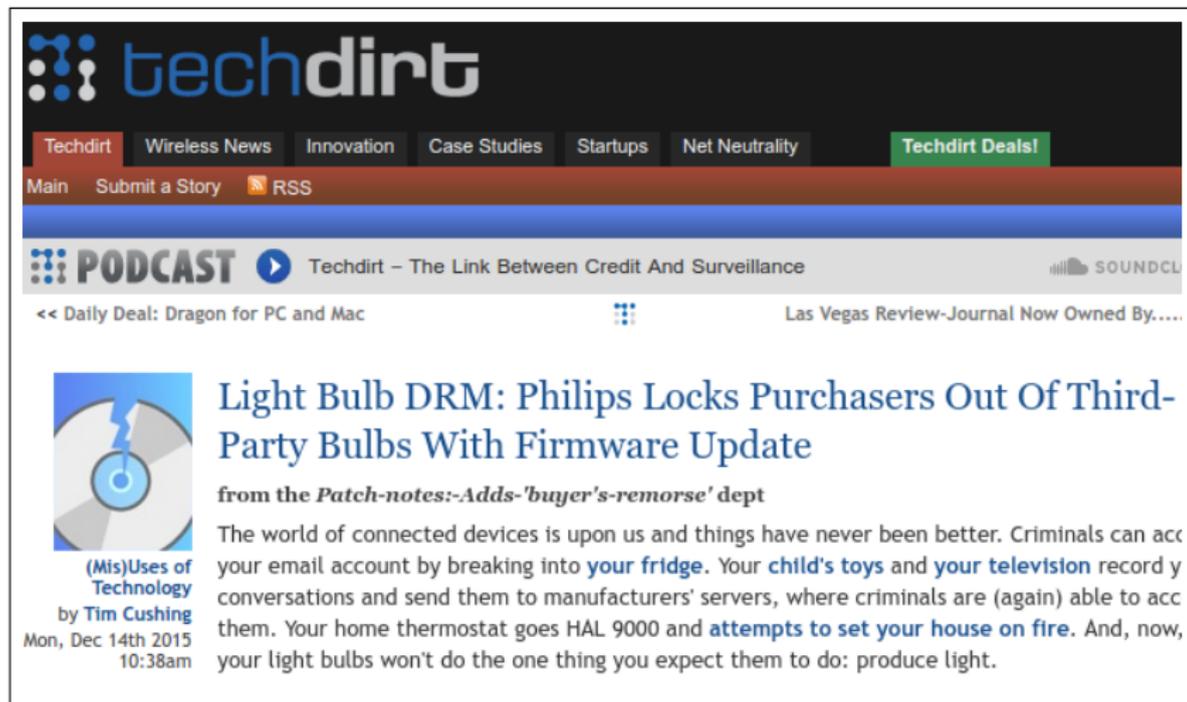
- ▶ Data model at the right abstraction level
- ▶ Standardized data types
- ▶ Global namespace

Lessons for BLE peripheral builders

- ▶ Don't rely on exclusive access for semantics
- ▶ One GATT transaction per application transaction

<https://github.com/helena-project/beetle>

Are corporations just evil?



The image is a screenshot of a Techdirt website article. At the top left is the Techdirt logo, consisting of a grid of blue dots followed by the word "techdirt" in a blue sans-serif font. Below the logo is a navigation bar with several tabs: "Techdirt" (highlighted in red), "Wireless News", "Innovation", "Case Studies", "Startups", "Net Neutrality", and "Techdirt Deals!" (highlighted in green). Underneath the navigation bar are links for "Main", "Submit a Story", and "RSS". A blue horizontal bar separates the navigation from the content area. Below this bar is a "PODCAST" section with a play button icon and the text "Techdirt - The Link Between Credit And Surveillance". To the right of this text is a "SOUNDCL" icon. Below the podcast section are two links: "<< Daily Deal: Dragon for PC and Mac" and "Las Vegas Review-Journal Now Owned By....". The main article features a square image of a light bulb with a blue lightning bolt striking it, set against a circular background. To the right of the image is the article title "Light Bulb DRM: Philips Locks Purchasers Out Of Third-Party Bulbs With Firmware Update" in a large blue font. Below the title is the byline "from the Patch-notes:-Adds-'buyer's-remorse' dept". The main body of the article is a paragraph of text starting with "The world of connected devices is upon us and things have never been better. Criminals can acc your email account by breaking into your fridge. Your child's toys and your television record y conversations and send them to manufacturers' servers, where criminals are (again) able to acc them. Your home thermostat goes HAL 9000 and attempts to set your house on fire. And, now, your light bulbs won't do the one thing you expect them to do: produce light." To the left of the article text is a vertical sidebar containing the text "(Mis)Uses of Technology by Tim Cushing" and the date and time "Mon, Dec 14th 2015 10:38am".

techdirt

Techdirt Wireless News Innovation Case Studies Startups Net Neutrality **Techdirt Deals!**

Main Submit a Story RSS

PODCAST Techdirt - The Link Between Credit And Surveillance SOUNDCL

<< Daily Deal: Dragon for PC and Mac Las Vegas Review-Journal Now Owned By....



Light Bulb DRM: Philips Locks Purchasers Out Of Third-Party Bulbs With Firmware Update

from the *Patch-notes:-Adds-'buyer's-remorse' dept*

The world of connected devices is upon us and things have never been better. Criminals can acc your email account by breaking into **your fridge**. Your **child's toys** and **your television** record y conversations and send them to manufacturers' servers, where criminals are (again) able to acc them. Your home thermostat goes HAL 9000 and **attempts to set your house on fire**. And, now, your light bulbs won't do the one thing you expect them to do: produce light.

(Mis)Uses of Technology
by Tim Cushing
Mon, Dec 14th 2015
10:38am

Are corporations just evil?



SEARCH



INNOVATION

SECURITY

DATA CENTERS

MORE ▾

NEWSLETTERS

ALL WRITERS

MUST READ [WHAT HAPPENS TO THOSE FREE WINDOWS 10 UPGRADES AFTER JULY 29?](#)

Nest to brick Revolv smart hubs on Sunday, and there's nothing owners can do about it

If you own a Revolv smart hub, then Sunday is the day that Nest will pull the plug on it, and you can kiss your \$300 gadget goodbye.



By [Adrian Kingsley-Hughes](#) for [Hardware 2.0](#) | June 17, 2016 -- 19:00 GMT (12:00 PDT) | Topic: [Google](#)

[\(mis\)uses of Technology](#)

by [Tim Cushing](#)

Mon, Dec 14th 2015
10:38am

your smart account by breaking into [your fridge](#), [your child's toys](#) and [your television records](#) conversations and send them to manufacturers' servers, where criminals are (again) able to access them. Your home thermostat goes HAL 9000 and [attempts to set your house on fire](#). And, now, your light bulbs won't do the one thing you expect them to do: produce light.

Are corporations just evil?

The image is a screenshot of a ZDNet news article. At the top, the ZDNet logo is on the left, and navigation links for SEARCH, INNOVATION, SECURITY, DATA CENTERS, MORE, NEWSLETTERS, and ALL WRITERS are on the right. Below the navigation bar, the article's byline reads 'bingbing / CORY DOCTOROW / 7:00 AM THU'. The main headline is 'GM says you don't own your car, you just license it'. Below the headline is a photograph of a white SUV parked outdoors. A yellow traffic cone is placed on the ground in front of the front wheel of the car. The background shows trees and a utility pole. To the right of the article, there are fragments of other text, including 'g owners', 'will pull', and 'And, now,'.

ZDNet

SEARCH INNOVATION SECURITY DATA CENTERS MORE NEWSLETTERS ALL WRITERS

bingbing / CORY DOCTOROW / 7:00 AM THU

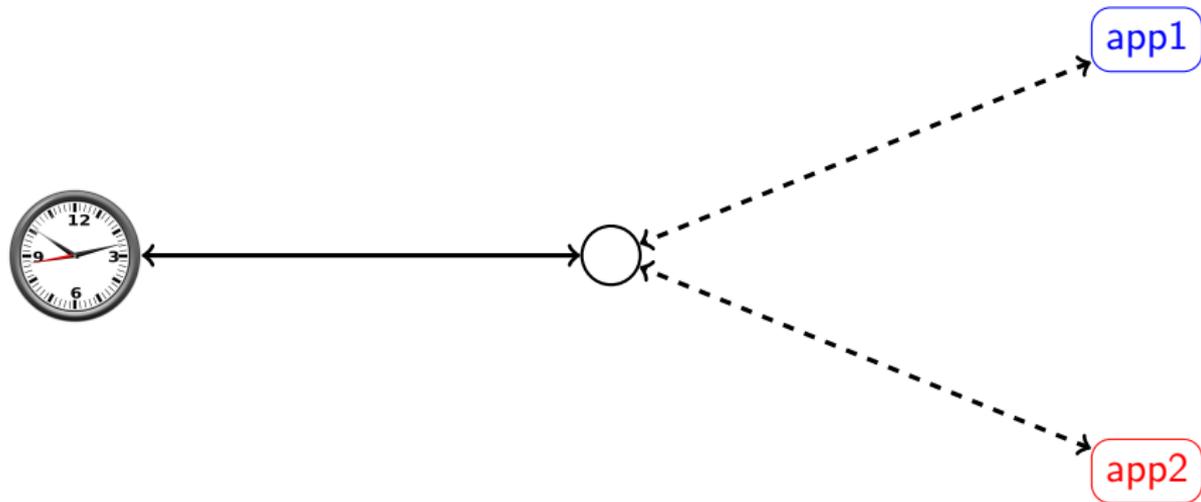
GM says you don't own your car, you just license it

g owners

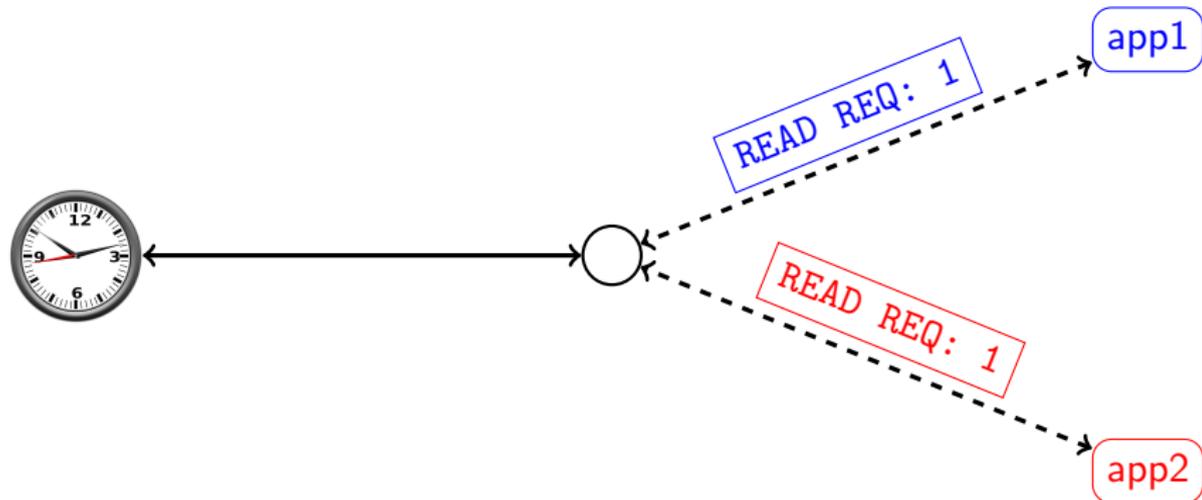
will pull

And, now,

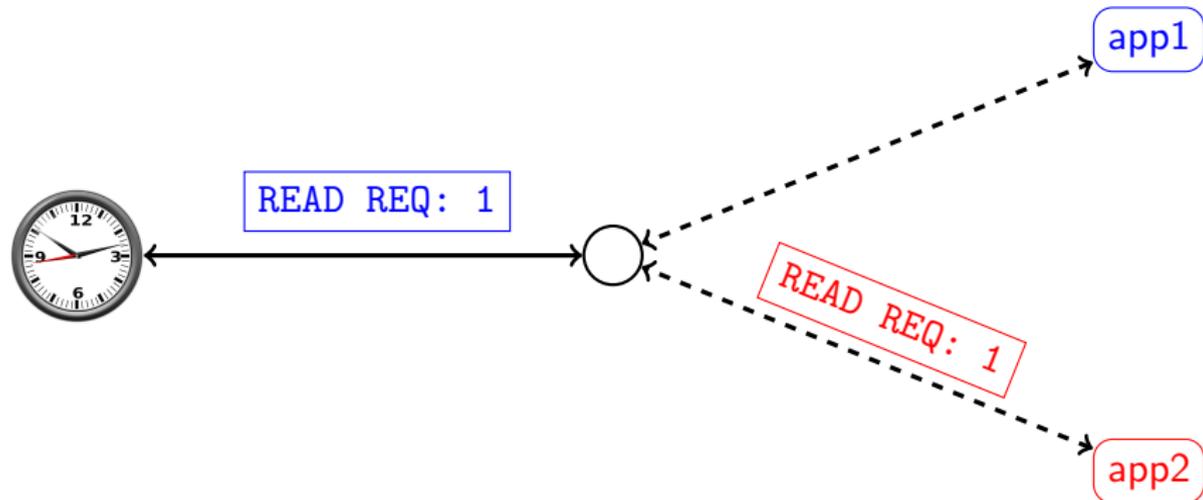
Attribute Caching



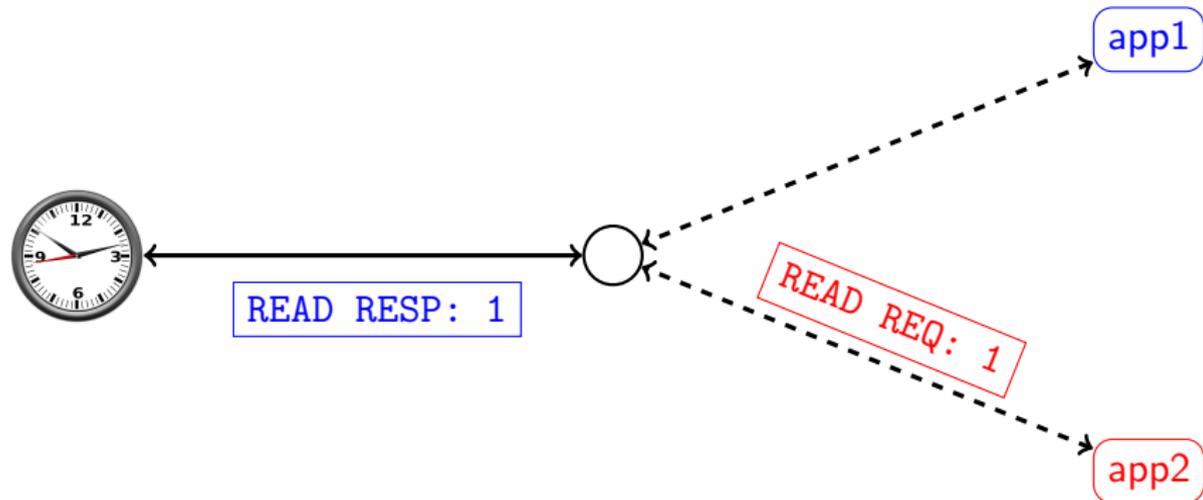
Attribute Caching



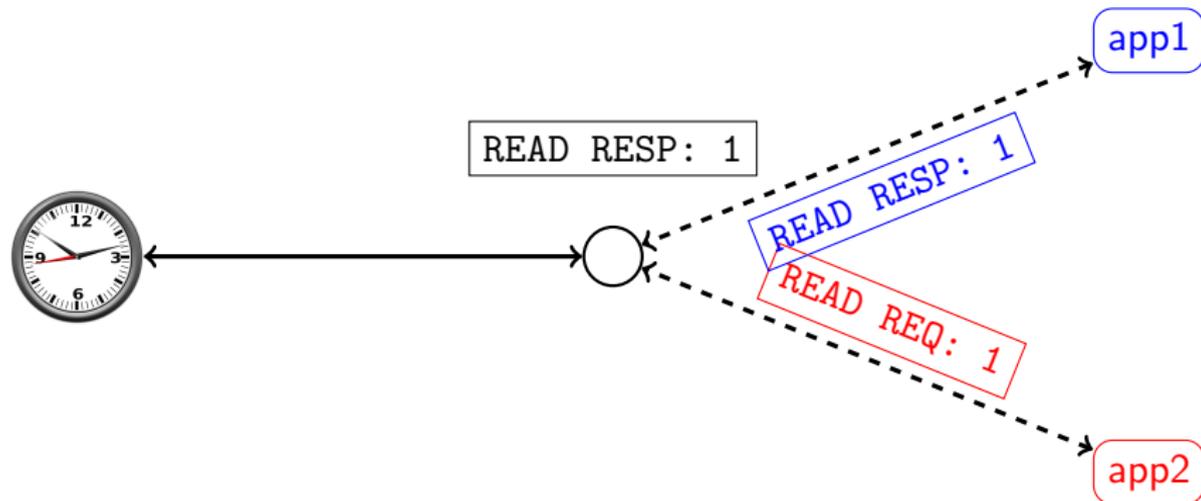
Attribute Caching



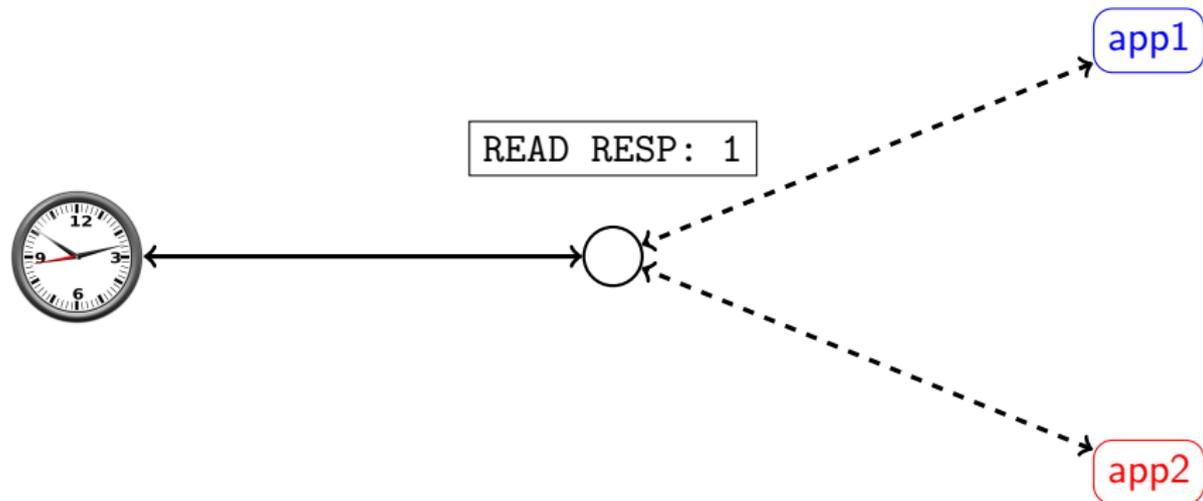
Attribute Caching



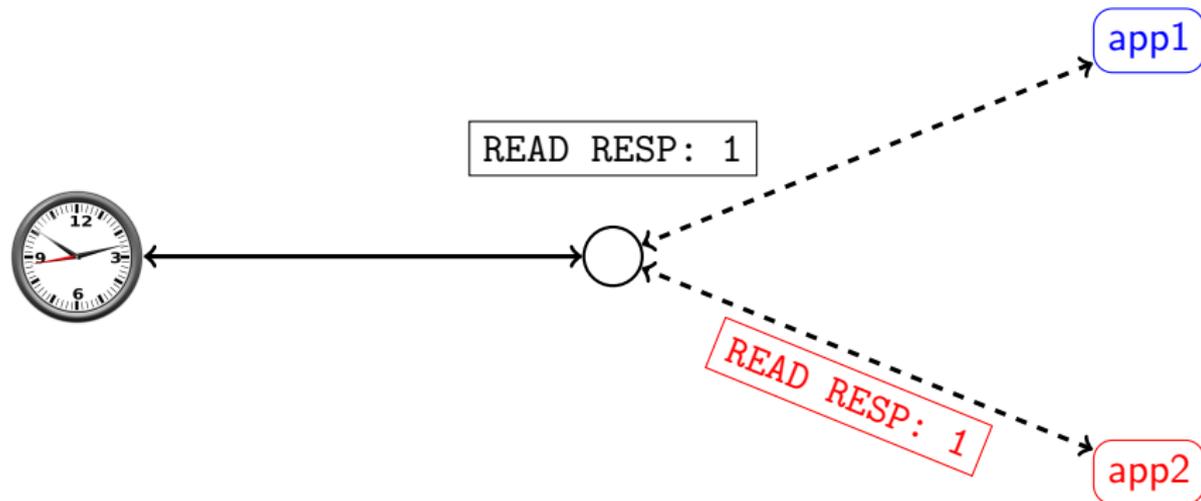
Attribute Caching



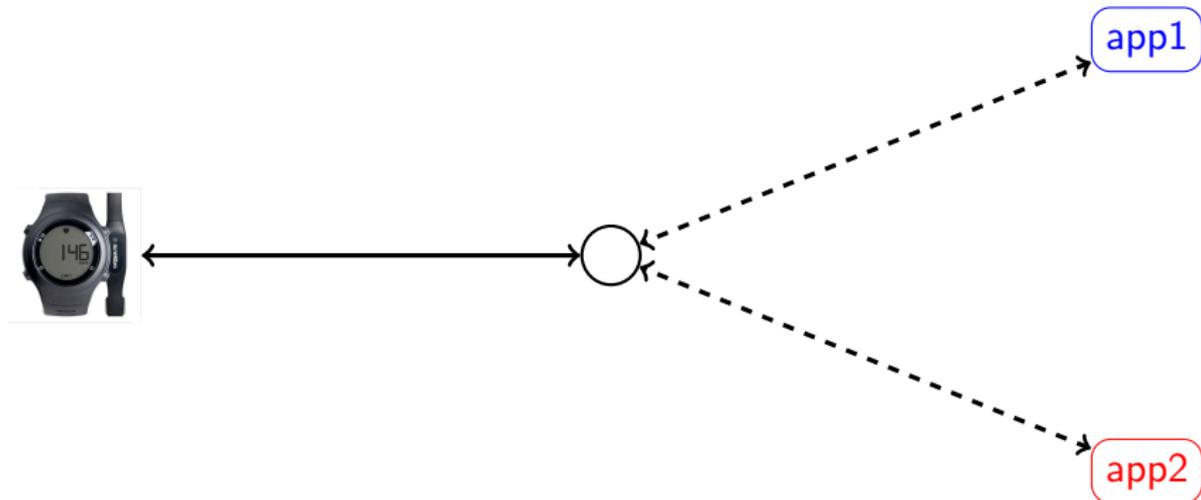
Attribute Caching



Attribute Caching

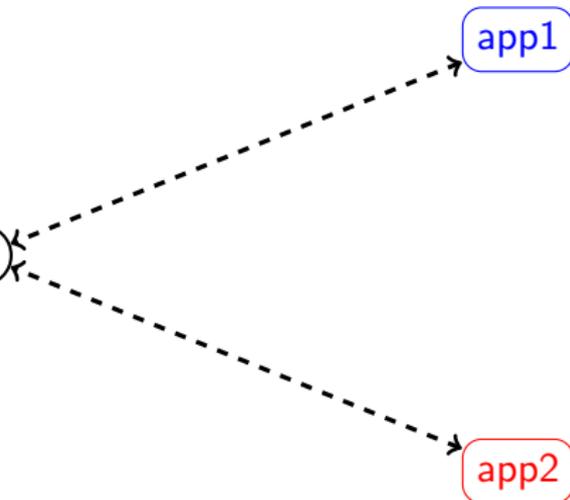


Handling Subscriptions

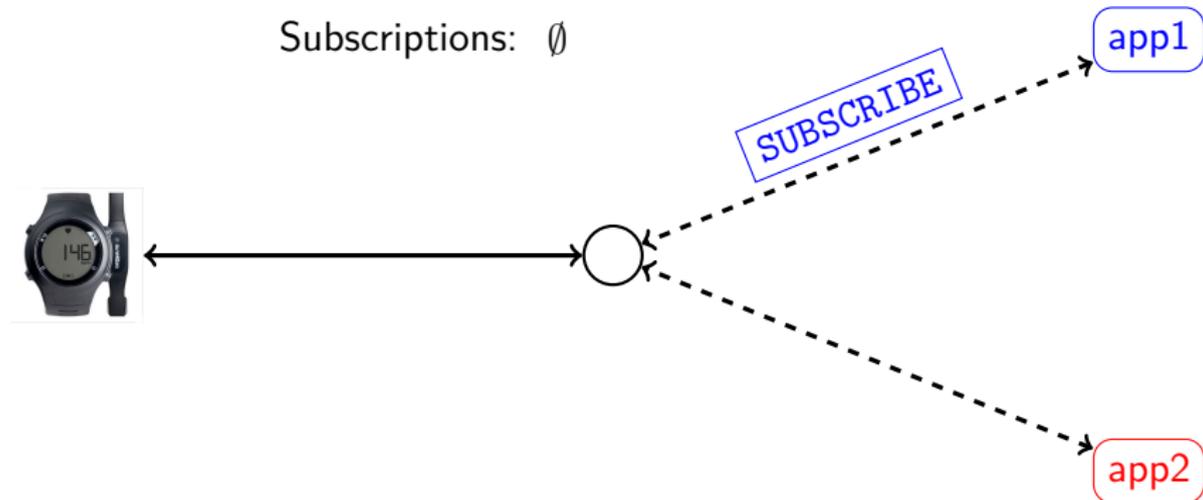


Handling Subscriptions

Subscriptions: \emptyset

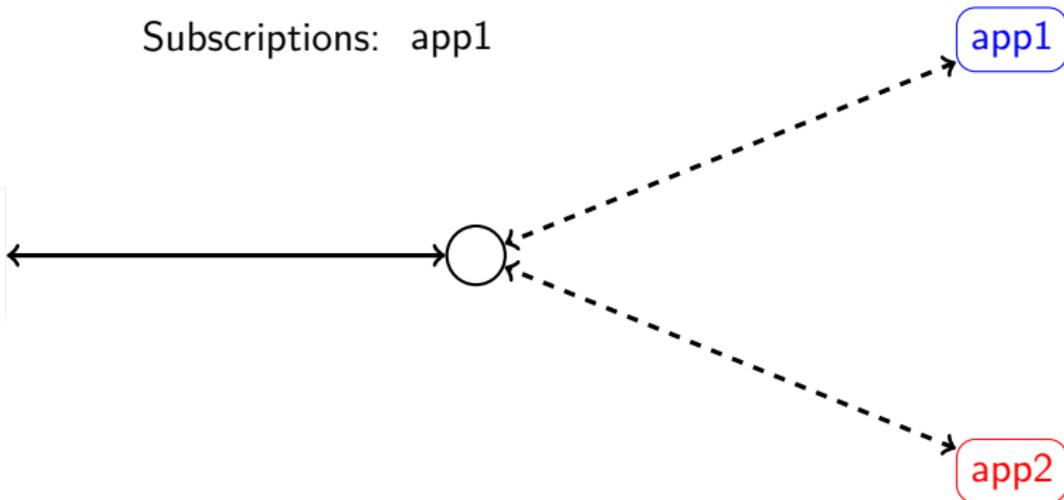


Handling Subscriptions

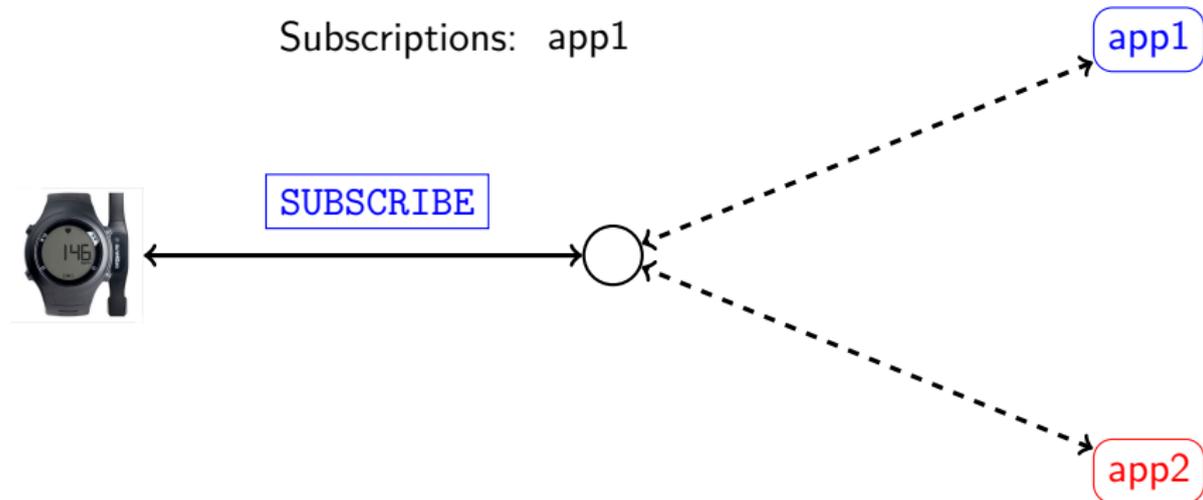


Handling Subscriptions

Subscriptions: app1

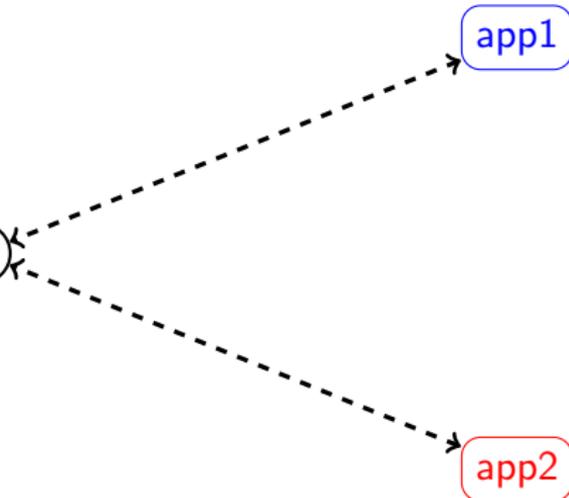


Handling Subscriptions

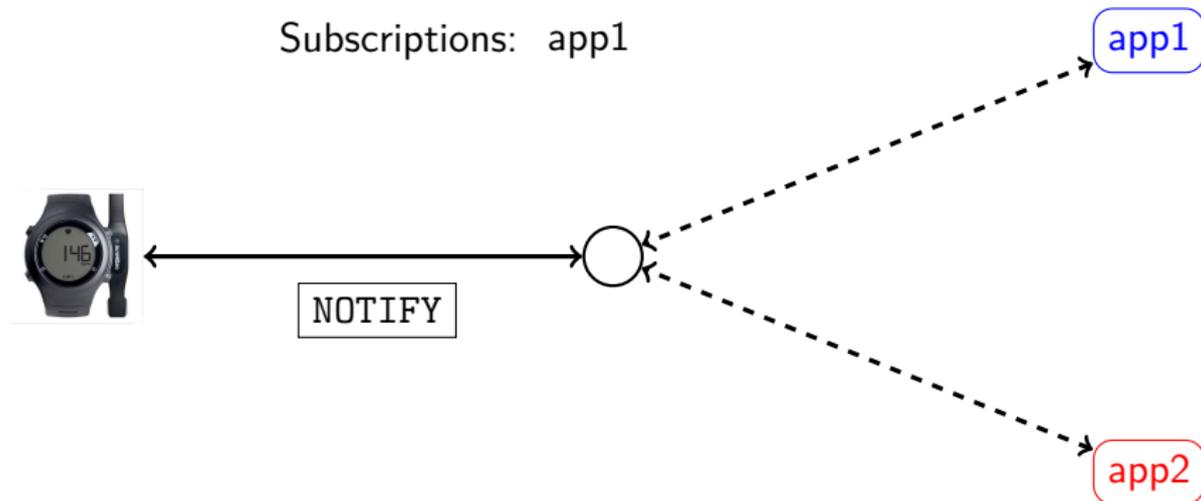


Handling Subscriptions

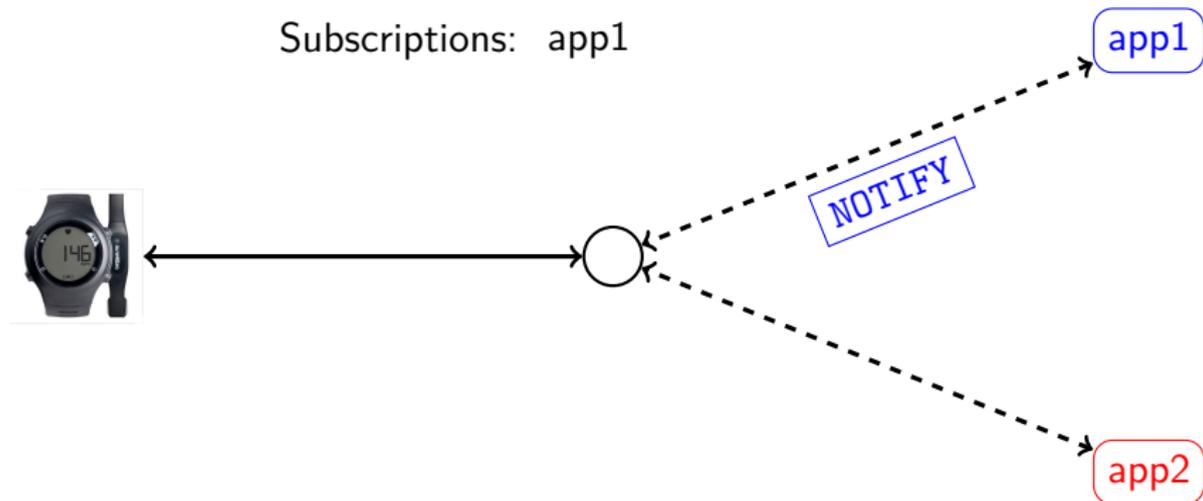
Subscriptions: app1



Handling Subscriptions

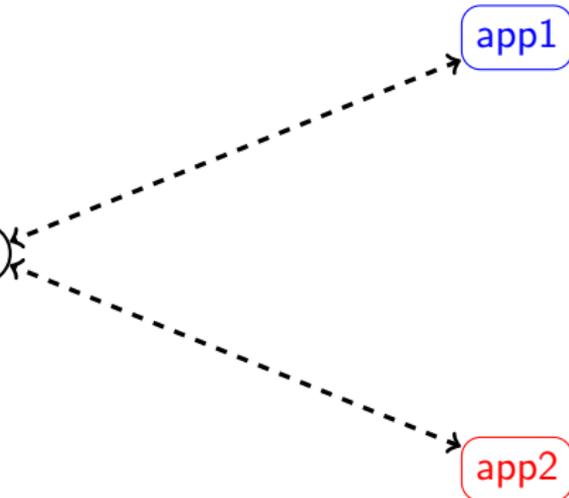


Handling Subscriptions

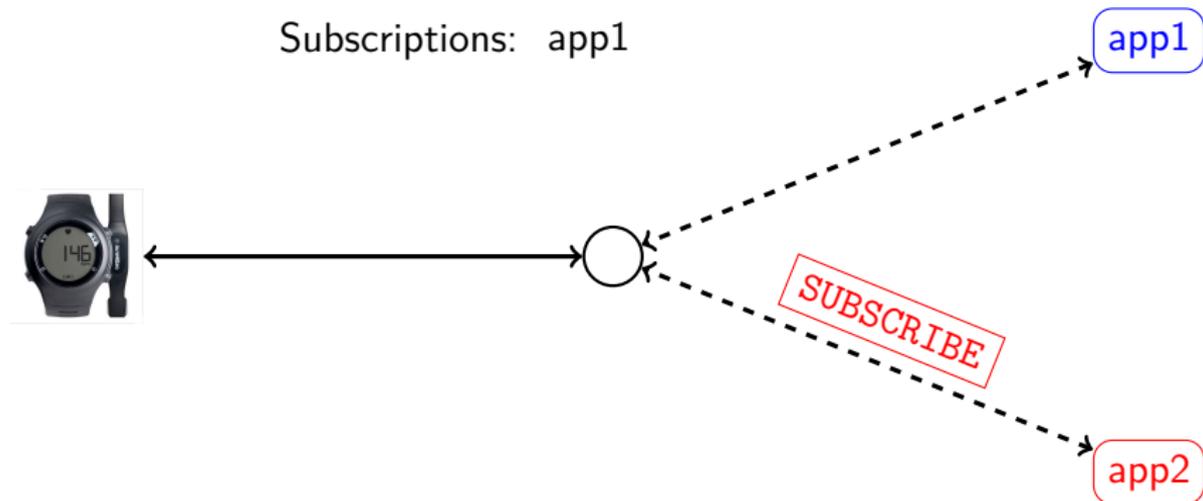


Handling Subscriptions

Subscriptions: app1

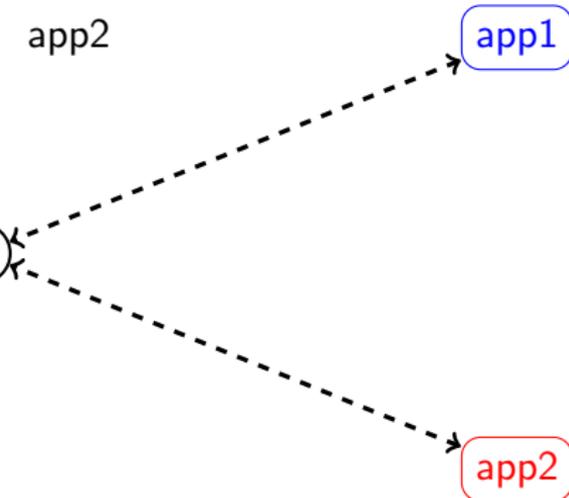


Handling Subscriptions



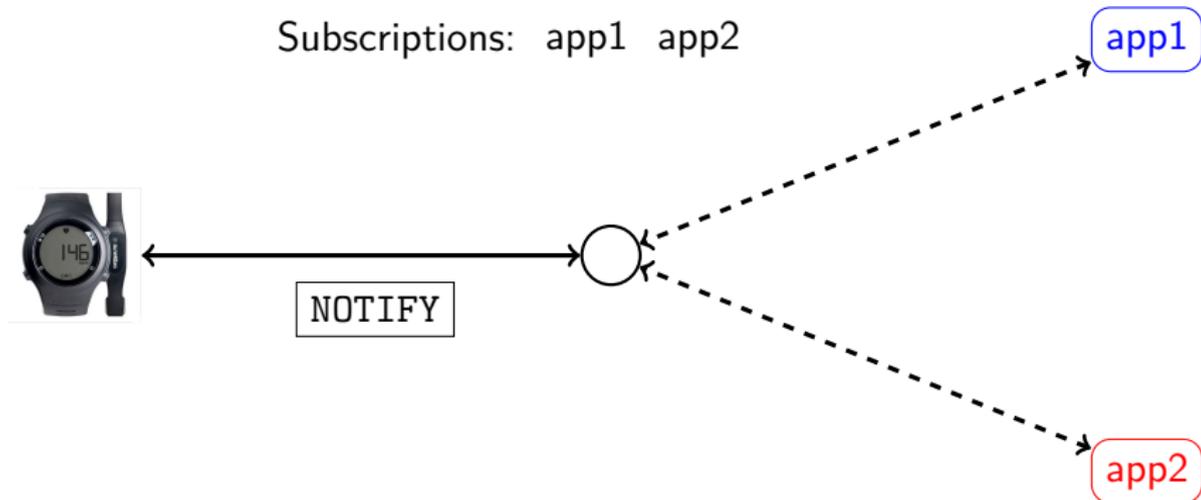
Handling Subscriptions

Subscriptions: app1 app2



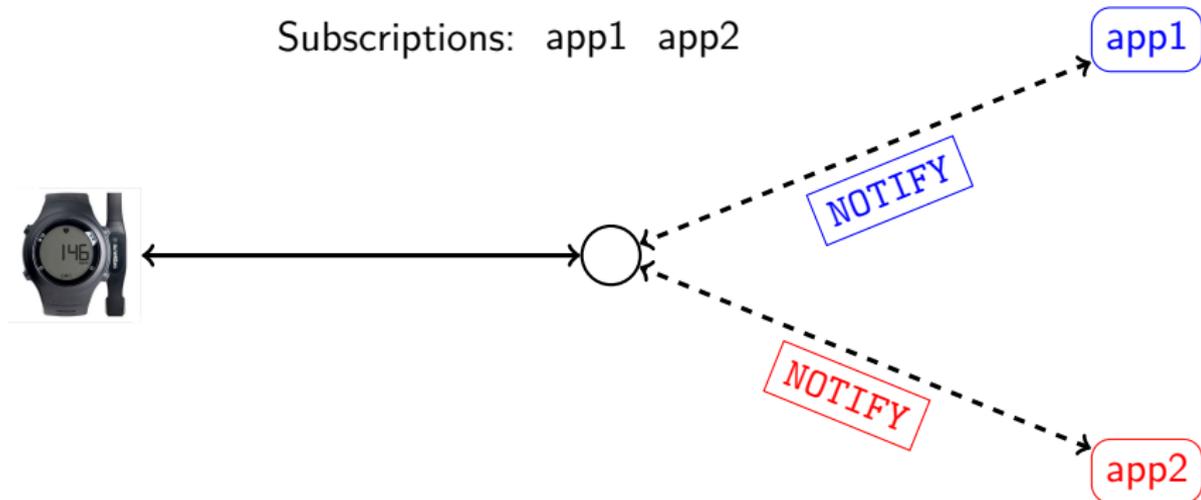
Handling Subscriptions

Subscriptions: app1 app2



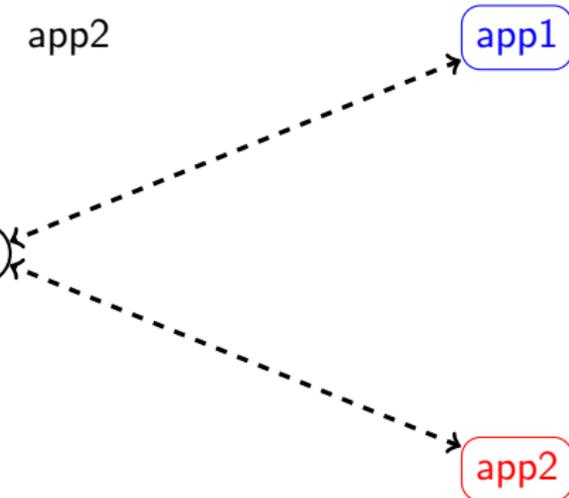
Handling Subscriptions

Subscriptions: app1 app2



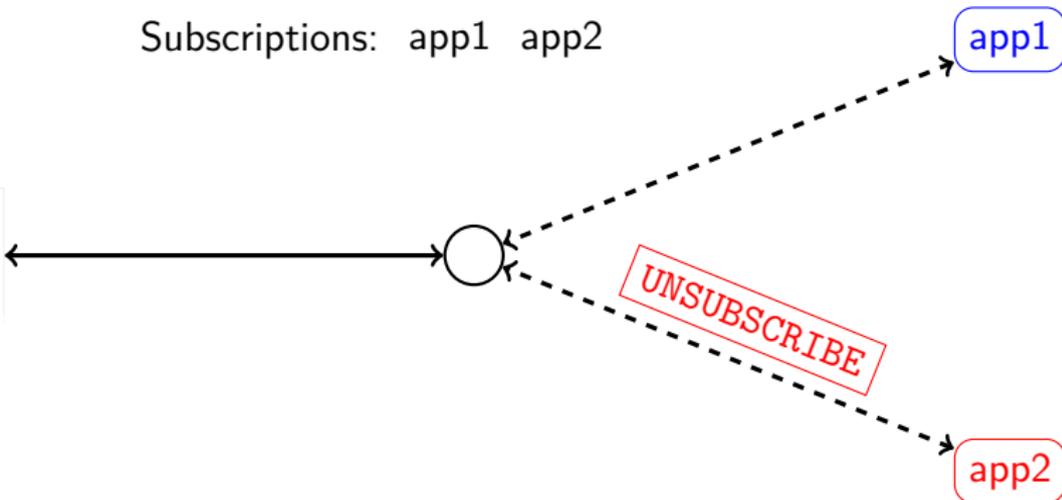
Handling Subscriptions

Subscriptions: app1 app2

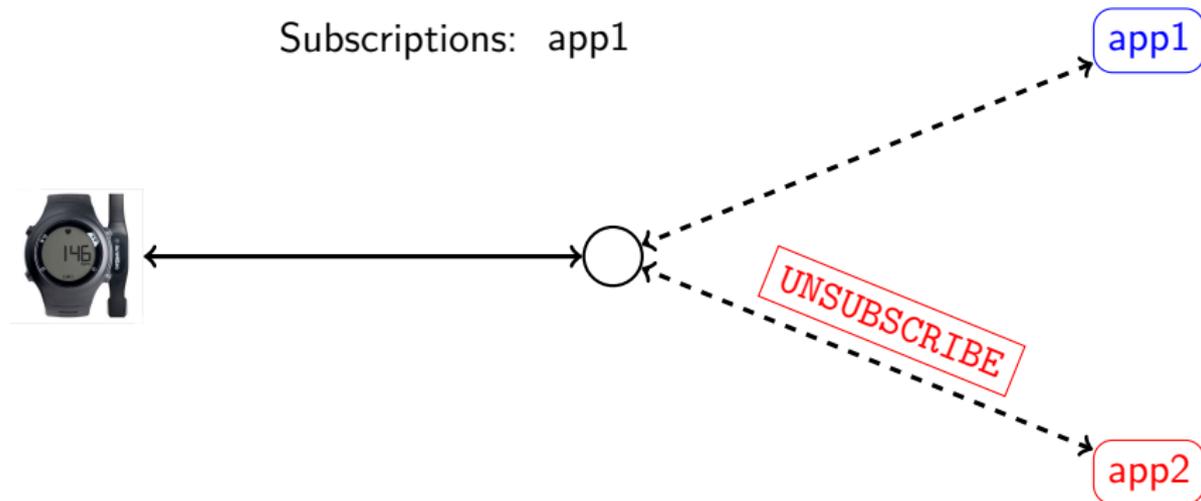


Handling Subscriptions

Subscriptions: app1 app2

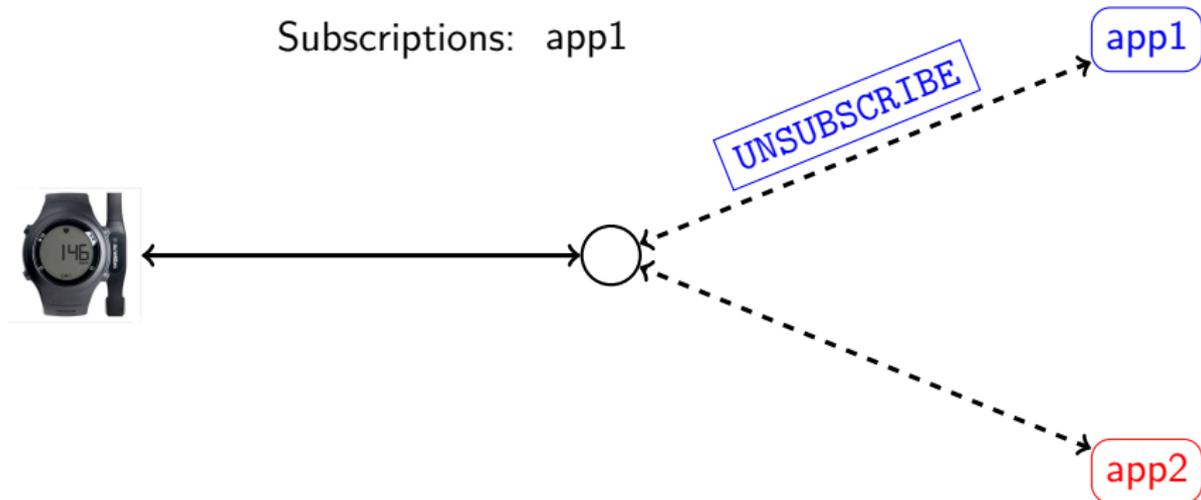


Handling Subscriptions



Handling Subscriptions

Subscriptions: app1



Handling Subscriptions

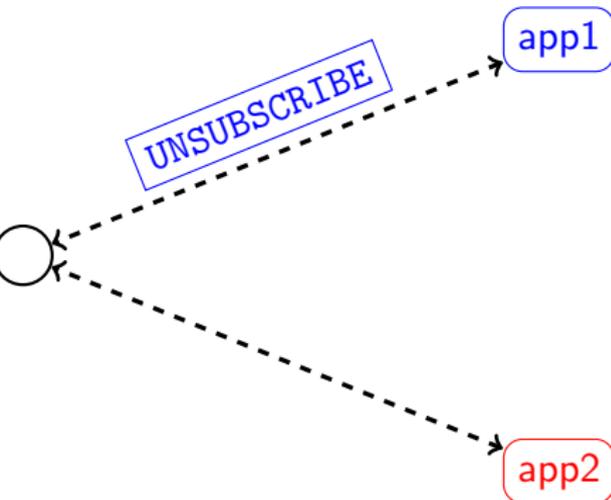
Subscriptions: \emptyset



UNSUBSCRIBE

app1

app2

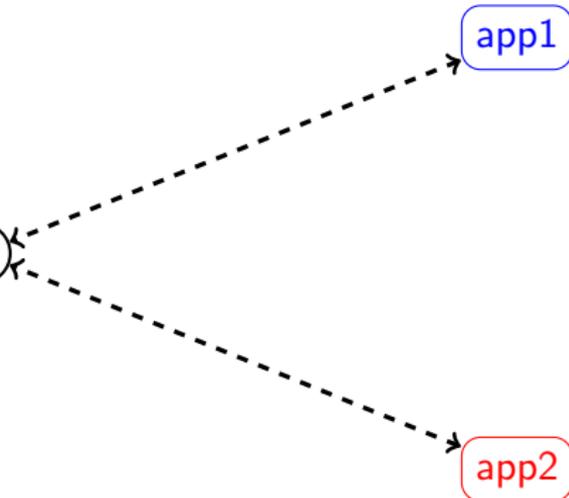


Handling Subscriptions

Subscriptions: \emptyset



UNSUBSCRIBE



Performance: Caching

