# Mobile Information Systems

# Lecture 08: UbiComp & IoT

© 2015-24 Dr. Florian Echtler
Bauhaus-Universität Weimar
Aalborg University

# Ubiquitous Computing

Source (FU): Mark Weiser, “The Computer for the 21st Century”, 1991

- Mark Weiser, 1991: “The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.”
- Proposes 3 device classes:
  - Tabs: wearable centimetre sized devices
  - Pads: hand-held decimetre-sized devices
  - Boards: metre sized interactive display devices.

→ Original vision has already (mostly) arrived.

# Ubiquitous Computing (2)

- … or has it?
  - Ubiquitous computing not just about devices …
  - … but also about interaction (or lack thereof)
- Also {calm | ambient | pervasive} computing
  → implies less/no manual setup effort
- Ever tried to use more than one Bluetooth device at once?

→ Not *quite* there yet after all.

# “Internet of Things” (IoT)

- Mostly a (widely/over-used) marketing term
- Core idea: put connectivity *everywhere*
- Basic concept similar to UbiComp:
  - Less focus on personal/interactive devices
  - More focus on “smart things” & sensor networks
  - E.g. light bulb, fridge, trash can, water meter…
  - Also: “Industry 4.0”, “Factory of the Future”

# “Internet of Things” (IoT) (2)

- Stated goals:
  - Automate mundane, everyday tasks
  - Increase energy/resource efficiency
  - “Smarter” logistics, e.g. in factories
- Other goals:
  - Sell more wireless sensor modules?
  - Gather more data about consumers?
  - E.g. wireless power meter → possible to infer movie being currently watched! (How?)

# Big issues for UbiComp/IoT?

- Power/energy supply?
  - Imagine changing batteries across 1000s of sensors/ ”smart things”... → energy harvesting?
- Interaction concepts?
  - People already struggle with synchronizing *two* devices → how to manage huge networks?
- Privacy & security?
  - Even more massive amounts of private data that requires adequate protection
- Standards (or lack thereof)

# UbiComp/IoT Technologies

- Wearables & interaction concepts
- Sensor & mesh networks
- Personal area networks (BTLE, NFC)

# Wearables & interaction concepts

- “Wearable” = any body-worn, hands-free device
  - Smartwatches, fitness trackers
  - Smart glasses, e.g. Google Glass
  - Headsets/headphones?
- Require new interaction concepts
  - E.g. small screen or no screen at all

    → use swipe/shake gestures

    → use voice commands

# Smartwatches (1)

Image sources (GFDL): https://en.wikipedia.org/.../Fossil_Wrist_PDA, (PD): https://en.wikipedia.org/.../Moto360

- Not a new concept, exists since late 1990s
- Recent popularity due to …
  - Companion device for smartphone
    → less complex hardware & power supply
  - Better/more sensors, e.g. motion, heart rate, …
  - Improved screens (e.g. round LCDs)
- Problems:
  - Battery lifetime
  - Size

# Smartwatches (2)

- Hardware
  - Surprisingly powerful (1 GHz quad-core, 4 GB ROM)
  - Bluetooth LE + (sometimes) WiFi
- Software
  - Android Wear (Android derivative)
  - Various proprietary OS (iOS, Tizen, …)
  - Native notification & app support:
    - iOS device + Apple Watch
    - Android device + Android Wear

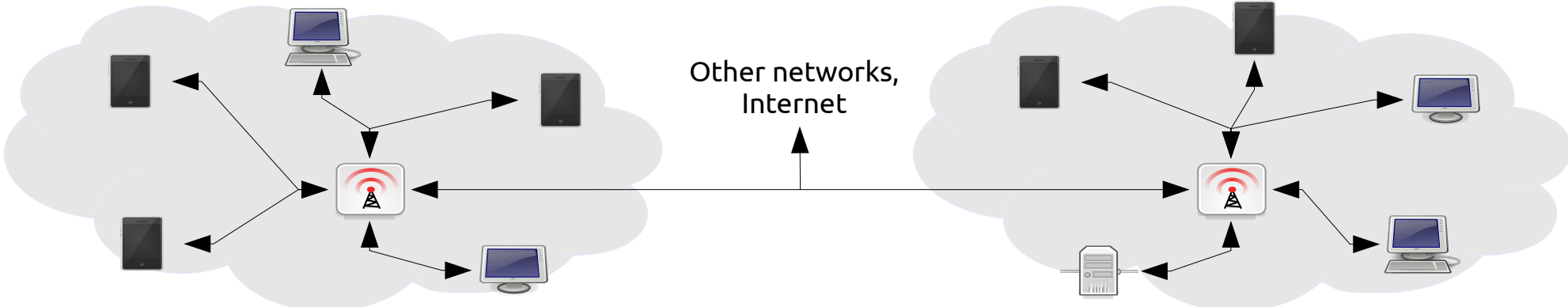
# Smartwatches (3)

- New interaction concepts:
  - Rough swipes, motion gestures (no pinch-zoom :-)
  - Interaction with smartphone: e.g. trace in-air gestures after touch lifted
- Usage scenarios:
  - Notifications & quick responses
  - Data logging (body state/movement/sleep)
  - … other ideas … ?

# Sensor & mesh networks (1)

Image source (CC): http://tango.freedesktop.org/

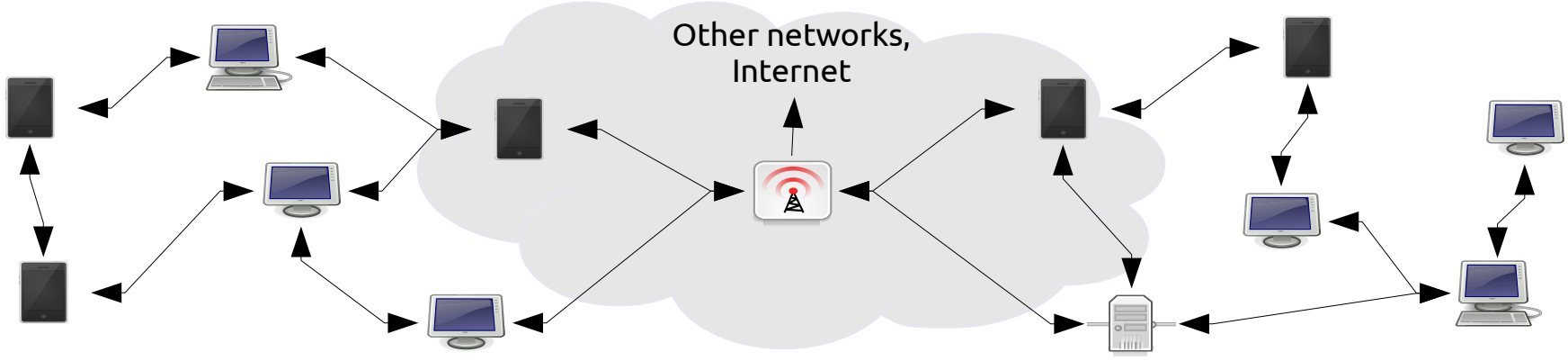
- "Regular" networks: star/tree topology
  - Central hubs for each segment (wired or wireless)
- Problems for sensors & IoT devices
  - Low transmission power → short range
  - Would require (many) additional hubs/gateways?



# Sensor & mesh networks (2)

Image source (CC): http://tango.freedesktop.org/

- Alternative: mesh networks
  - Each device also acts as hub/relay
  - Data is forwarded across several “hops”
  - Topology can change dynamically



# Sensor & mesh networks (3)

- Main forwarding strategies:
  - Flooding, re-broadcasting (problems?)
  - Routing – on-demand: e.g. Ad hoc On-Demand Distance Vector (AODV)
  - Routing – pro-active, e.g. Optimized Link State Routing (OLSR), B.A.T.M.A.N. (cf. Freifunk network)
- Current implementations:
  - ZigBee (IEEE 802.15.4)
  - Bluetooth LE (since 5.1)
  - WiFi-based (Freifunk)

# Sensor & mesh networks (4)

- Alternative: LPWAN (Low Power WAN)
  - Relatively long range (1-10 km)
  - Very low bandwidth (< 50 kBit/s)
  - Also uses ISM bands
- Current standards: LoRaWAN, Weightless, WiFi HaLow, …
- Not (yet) widely used
- Intended for smart meters, street lamps, etc.

# Personal Area Network (WPAN)

- Originally IrDA, later Bluetooth (see lecture 3)
- Goal: communication with personal peripherals
- Disadvantages:
  - High power draw (on par with WiFi/cellular)
  - Complex setup procedures (pairing, PIN codes etc.)
- Alternative: Bluetooth Low Energy (BLE/BTLE), aka Bluetooth Smart
  - Also available for medium-area mesh networks

# Bluetooth Low Energy (1)

Image source (FU): http://www.bluetooth.com/Pages/Bluetooth-Brand.aspx (Logo)

- Little in common with “classic” Bluetooth
  - Same frequency band (2.4 GHz ISM)
  - Similar modulation → no hardware change
  - Much smaller/less complex protocol stack
  - Part of Bluetooth specification v4.0
- Optimized for simple battery-powered sensors
  - Goal: months or years of battery lifetime
  - Maximum data rate 1 Mbit/sec

# Bluetooth Low Energy (2)

- 2 major roles: central or peripheral
  - Peripherals can …
    - Broadcast to all central devices
    - Unicast to one specific central device
  - Centrals can …
    - Open connections to peripherals
    - Be notified about value changes
- OS support (mobile):
  - Central role supported since Android 4.3, iOS 5
  - Peripheral since Android 5.0 (not all devices), iOS 6

# Bluetooth Low Energy (3)

- “Complexity” classes for peripherals:
  - Beacons (pure static broadcasts)
    - E.g. iBeacon: simply broadcasts own UUID
    - Additional data possible on request
  - Sensors (broad-/unicast with sensor data)
    - Multiple profiles: heart rate, activity, temperature, …
    - Notification support to avoid constant polling
  - Bidirectional communication
    - Not primarily designed for synchronous comm.
    - Mostly for setting sensor parameters etc.

# Bluetooth Low Energy (4)

- Power consumption
  - Highly dependent on advertising interval
  - nRF51822 SoC, CR2032 button cell, 1 s interval
    → estimate ~ 1 year of lifetime
  - Power management becomes very important
  - Modern SoCs have multiple peripherals
    that can be powered down individually

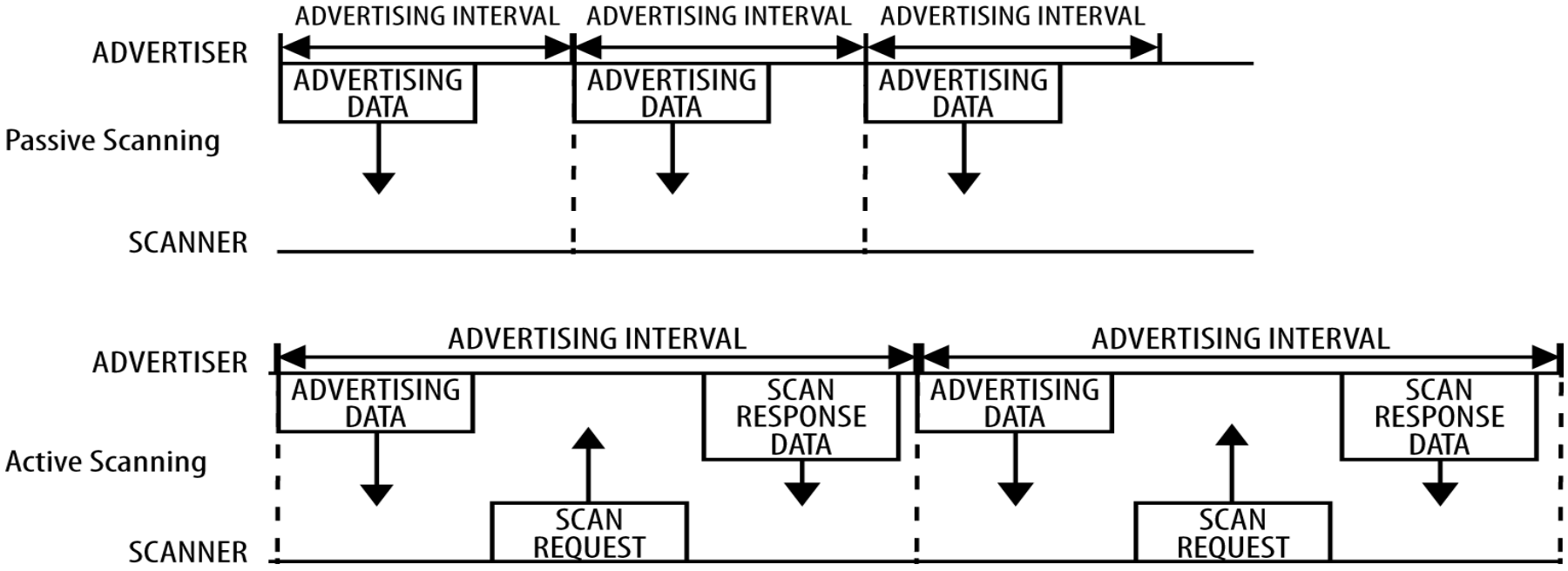
# BTLE Profiles/Protocols (1)

- GAP = Generic Advertising Profile
  - Up to 31 bytes advertisement broadcast
  - Up to 31 extra bytes on request by central
- GATT = Generic Attribute Profiles
  - Only available to one central at a time
  - 1+ *services*, containing 1+ *characteristics* each
  - Each s/c identified by global 16-bit UUID
  - Publish/subscribe model
    - Value change notifications, no constant data stream
    - Less “on” time for radio module → power savings

# BTLE Profiles/Protocols (2)

Image source (FU): Townsend et al., Getting Started with Bluetooth Low Energy, O'Reilly Media

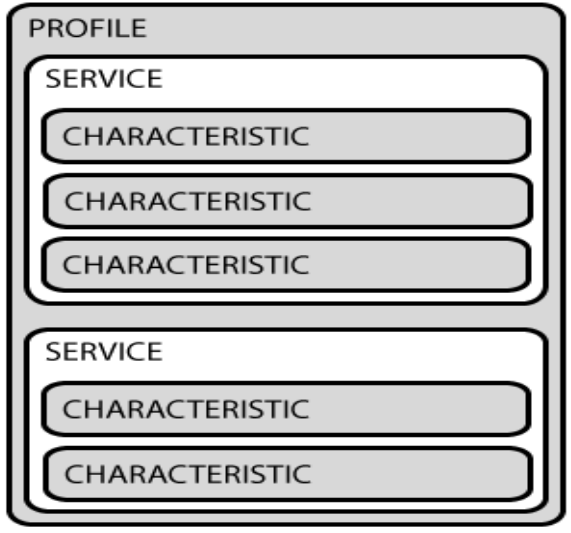
- GAP: Generic Access Profile
  - Advertising, discovery, connection establishment

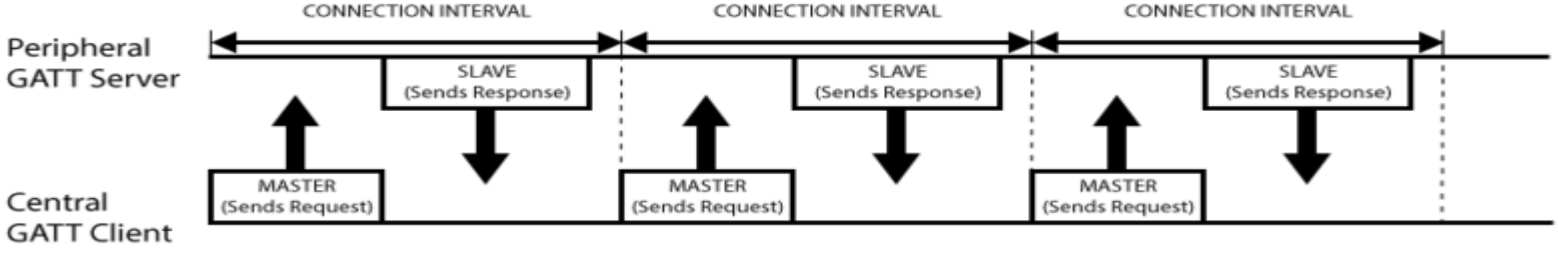


# BTLE Profiles/Protocols (3)

Image source (FU): https://learn.adafruit.com/introduction-to-bluetooth-low-energy/gatt

- GATT: Generic Attribute Profile
  - Main transport for “live” data
  - Extension of GAP
  - Profiles, services + characteristics (each with unique UUID)
  - Publish-subscribe model

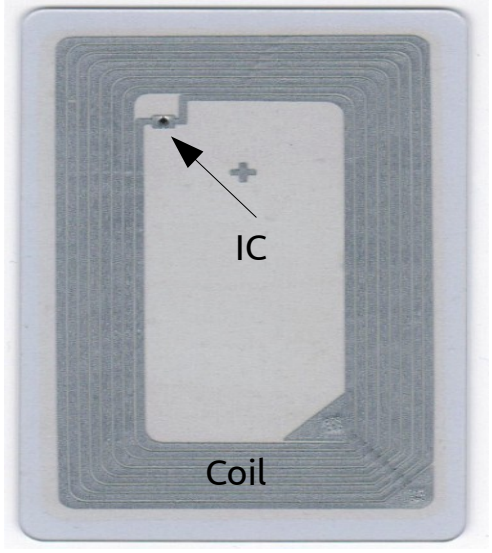


# Near Field Communication (NFC)

Image sources (FU): http://nfc-forum.org/ (Logo), (CC) own image

- Very simple devices, price down to ~ 0.10 €
  - Various form factors: sticker, token, card, glass capsule (implantable/injectable), …
  - Contain small IC + antenna coil
- Subclass of RFID (radio freq. ID)
- Power for tag provided by reader device through magnetic field
- Communication through EM field modulation (bi-directional!)



# Near Field Communication (NFC)

Image sources (FU): http://nfc-forum.org/ (Logo)

- Characteristics:
  - 13.56 MHz band, ~ 400 kBit/sec
  - Range ~ 2 cm with standard antenna
  - Storage: 137 byte – 80 kByte
- Variants:
  - Simple storage devices (cf. NDEF standard)
  - Smart cards with crypto functions (e.g. Mifare)
  - Java cards (user-programmable in Java)
  - Card emulation (device mimics card/token)

# Near Field Communication (NFC)

Image sources (FU): http://nfc-forum.org/ (Logo)

- Usage scenarios
  - URLs/contact data, e.g. in poster/business card
  - Security & access control (e.g. AAU student cards)
  - Mobile payment (some credit cards, Apple Pay)
  - Passports (lots of sensitive information)
  - Device-to-device (Android Beam)
- Directed antenna can increase range to ~1 m
  → personal data stolen without direct contact

# NFC Security

Image sources (FU): http://nfc-forum.org/ (Logo)

- Public tags:
  - should be write-protected (but often are not)
  - E.g. overwrite with malicious URL?
- Security measures
  - Simple/low-level:
    - Read and/or write keys for each data block
    - Can often be brute-forced or sniffed
  - Complex/high-level:
    - Dedicated crypto “apps” in NFC chip
    - Similar security concept to SIM card

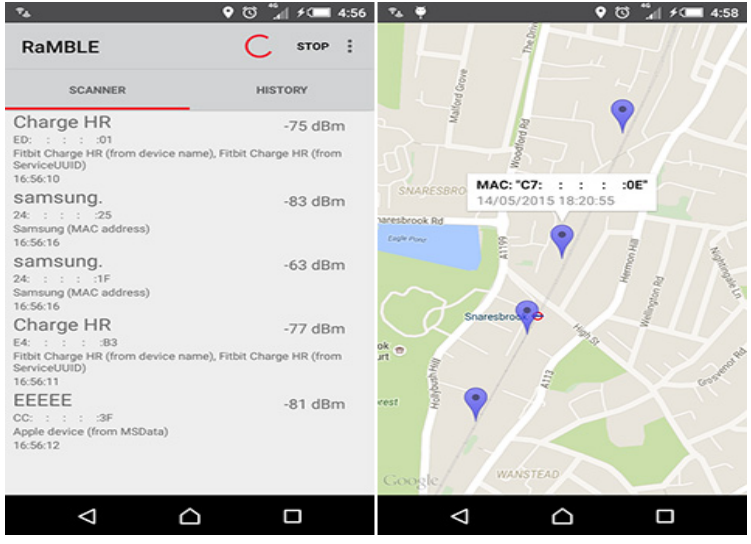
# UbiComp/IoT issue: energy supply

- Possible solution: energy harvesting?
- Many possible sources
  - Sunlight/environment light
  - Vibration & sound
  - Temperature differences
  - EM radiation (e.g. power lines, TV stations)
- Drawbacks:
  - Low efficiency (few 10-100 mW)
  - Energy storage (e.g. during night?)

# UbiComp/IoT issue: privacy

Image sources (FU): http://www.net-security.org/secworld.php?id=18422

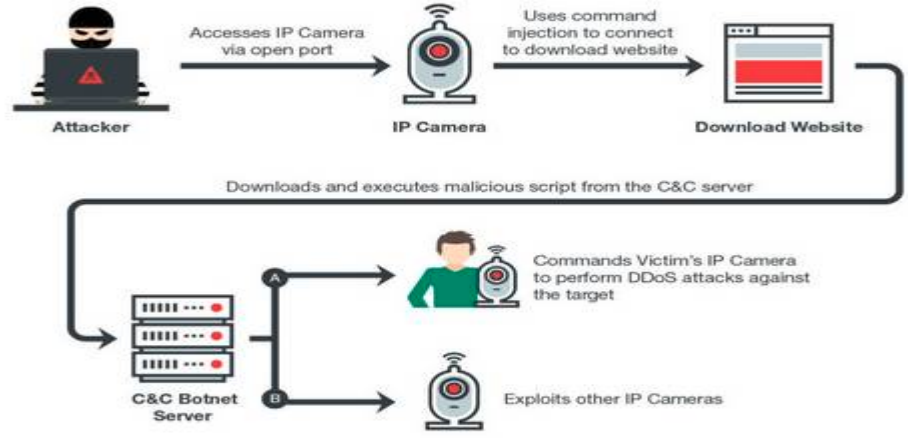
- Bluetooth LE devices: often broadcast-based
  - Implies public availability → enables tracking
  - Often leaks additional private data, e.g. pulse
  - MAC address *could* be random, but often isn't
- Classic tradeoff: security/ privacy ↔ ease of setup
- Danger of stalking (Apple AirTags, Google FindMy)



# UbiComp/IoT issue: security

Image source (FU): https://www.theregister.co.uk/2017/05/10/persirai_iot_botnet/

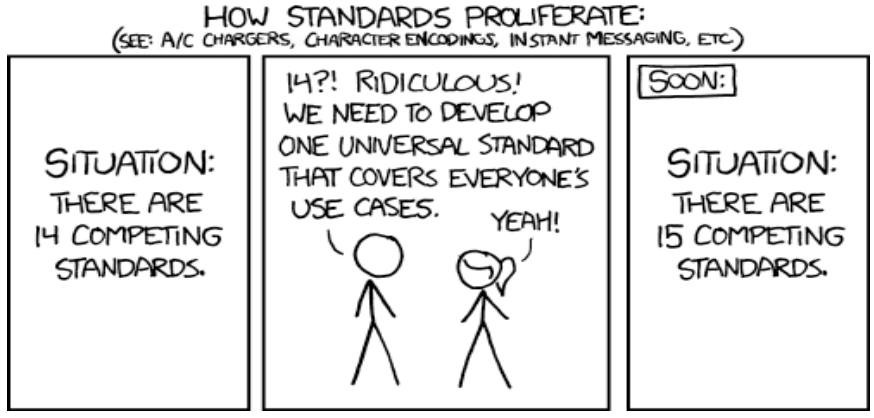
- Mobile phones: bad situation regarding patches, security updates etc.
- IoT devices: even *worse*
- Customer often won't even notice, so why bother?
- Problem: insecure devices on Internet → can be used as part of a *botnet*, execute DDOS attacks



# UbiComp/IoT issue: standards

Image sources (CC): https://xkcd.com/927/

- Current state: ~ 1 standard per manufacturer
  → e.g. light bulb A won't talk to control app B
  - Common ground: *sometimes* IP, more recently Matter Protocol
  - Mostly: wild mixture (HTTP, MQTT, Zigbee, …)
- "Universal" approach: URIBeacon/Physical Web
  - Every "smart thing" broadcasts an URL
  - Access/control via common web tools
  - Problem: mapping?



# The End