From Ubiquitous Computing to Internet of Everything: Challenges and Opportunities

Paul Patras

Hype or genuine evolution?

| 1988 | 1999 - 2002 | 2005 | 2009 | 2013 |

Ma EC, IoT — An Cisco – coins **Internet of Everything**   Things

"… "network of i "The Internet of Everything (IoE) brings together   ch new
pei to cars, from people, processes, data, and things to make   dio-frequency
fro These object; networked connections more relevant and   a world of
fin¡ Internet Prot valuable than ever before – turning information   ices (e.g.
tha complex syst into actions that create new capabilities, richer   >or, etc.) that
sor information f experiences, and unprecedented economic   nation
hig use actuators opportunity for businesses, individuals, and   heralding the
so ııuıng, so natu countries."   e internet (of
thinking about it. way ıoı compu data and people) acquires a new dimension to
                                                become an Internet of Things."
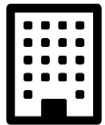
Numerous opportunities

Healthcare and assisted living

Transportation

Environment monitoring and agriculture

Smart buildings

Many more

Interconnecting many devices that exchange (big) data is challenging

How to model and predict the behaviour of complex systems?

How to ensure reliable connectivity and optimally share communictions infrastructure?

How to aggregate large data sets and exploit only context specific information in real-time?

How to preserve user privacy while achieving some utility from data processing?

How to ensure Internet-connected 'things' are secure and easy to use?

Different perspectives needed

UK researchers wrote Ubicomp manifesto in 2006[*] – some challenges facing ubiquitous system design still hold

Theoretical perspective: rigorous models that capture system behaviour at different levels of abstraction.

Engineering perspective: architectural and network challenges posed by large scale, heterogeneous, and dynamic nature.

Experience perspective: understand what principles underpin human-machine interaction and how a ubiquitous computing society might be shaped from a socio-technical perspective.

[*]D. Chalmers, M. Chalmers, J. Crowcroft, M. Kwiatkowska, R. Milner, E. O'Neill, T. Rodden, V. Sassone, M. Sloman, "Ubiquitous Computing: Experience, Design and Science", A Grand Challenge in Computing Research sponsored by the UK Computing Research Committee, 2006.

Application specific challenges

Computationally/energy constrained vs unconstrained devices
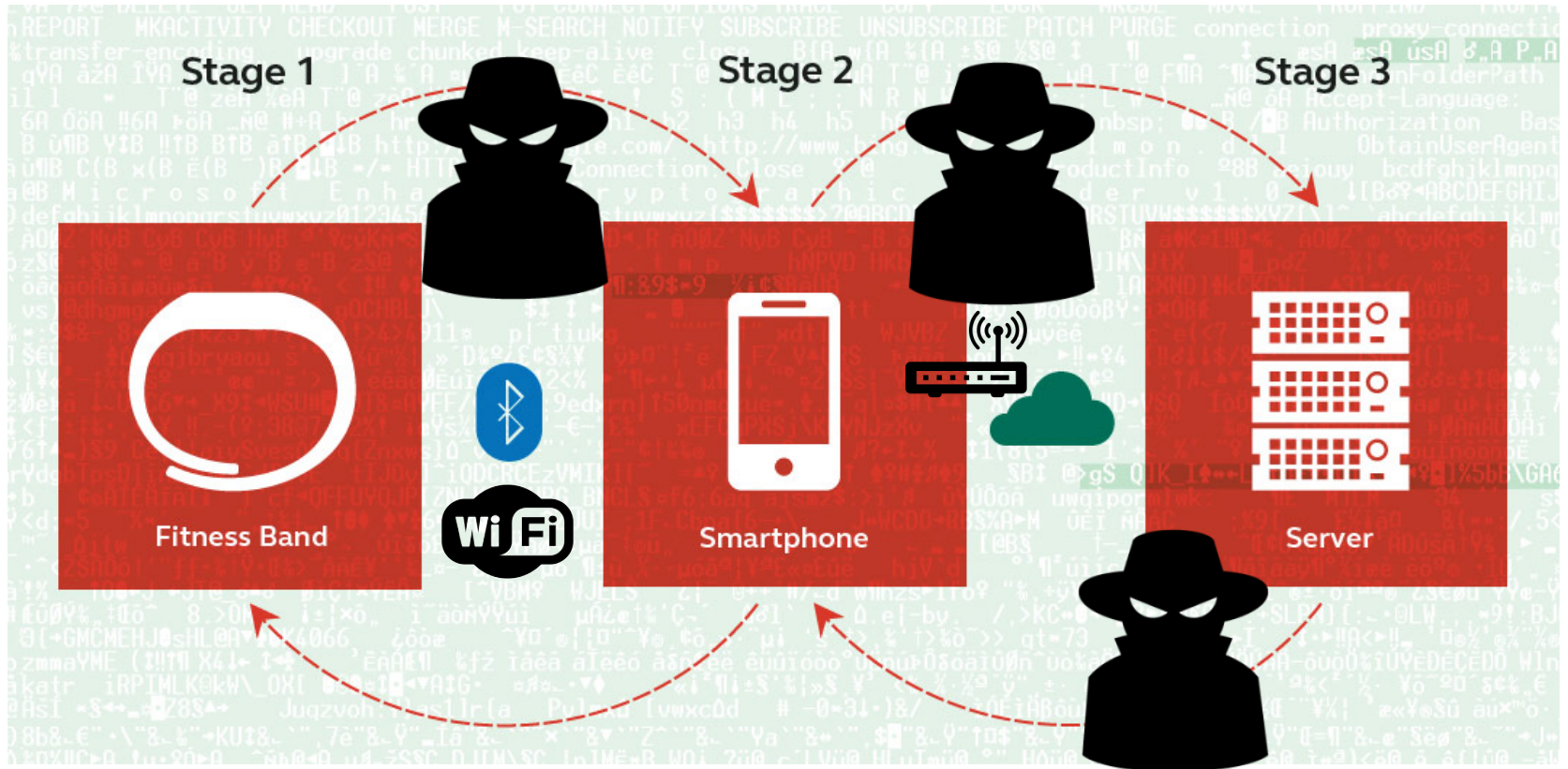
Communication type (decentralised vs scheduled and range (long vs short)

User interface (display, keys, touch, voice, gestures)

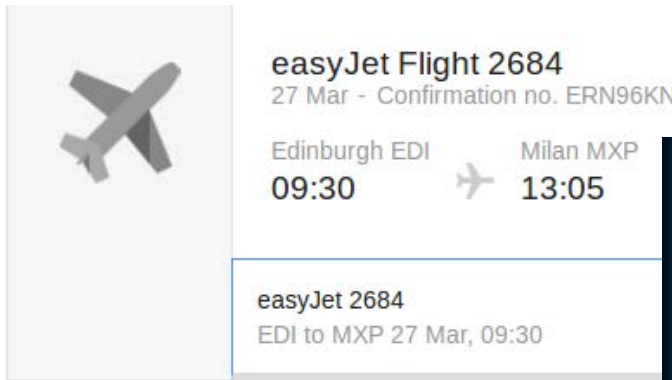# Example: Wristband fitness trackers (activity, sleep, heart rate monitoring)

Operation model

Surveillance at 10,000m

easyJet Flight 2684
27 Mar - Confirmation no. ERN96KN

Edinburgh EDI ✈ Milan MXP
09:30   13:05

easyJet 2684
EDI to MXP 27 Mar, 09:30

13 devices detected
within <1 minute

```
paul@batcat:~$ date
Mon 27 Mar 11:17:42 BST 2017
paul@batcat:~$ sudo hcitool lescan
[sudo] password for paul:
LE Scan ...
4F:FF:19:3D:F3:A6 (unknown)
48:94:29:F3:4E:BC (unknown)
69:20:9F:A7:78:06 (unknown)
E7:E4:B1:19:18:2B One
46:38:32:3A:5A:63 (unknown)
D8:CE:27:74:9B:FE Charge 2
E3:00:C9:B1:BA:52 Charge 2
E2:3E:C8:E6:7F:62 vívosmart HR
7B:BF:CD:46:4F:09 (unknown)
88:C6:26:01:05:08
77:D0:E4:0B:E3:2F (unknown)
4A:60:ED:6F:38:DB (unknown)
75:C1:8F:69:07:1C (unknown)
```

Security still an afterthought
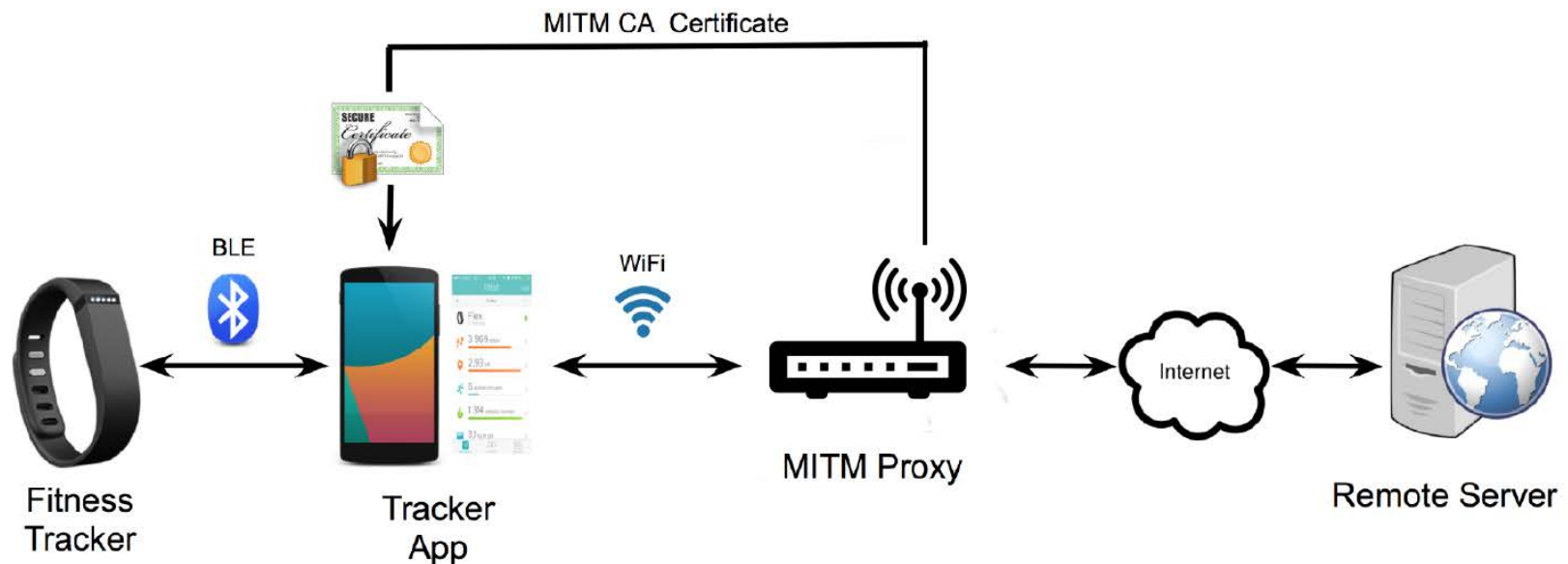
- Intercepting sensitive personal information is possible
- Injection of fake activity reports to gain rewards
- Compromising victim's personal statistics

H. Fereidooni, J. Classen, T. Spink, P. Patras, M. Miettinen, A.-R. Sadeghi, M. Hollick, M. Conti, "Breaking Fitness Records without Moving: Reverse Engineering and Spoofing Fitbit", to appear in Proc. RAID, Atlanta, GA, USA, Sept. 2017.

Smart Homes
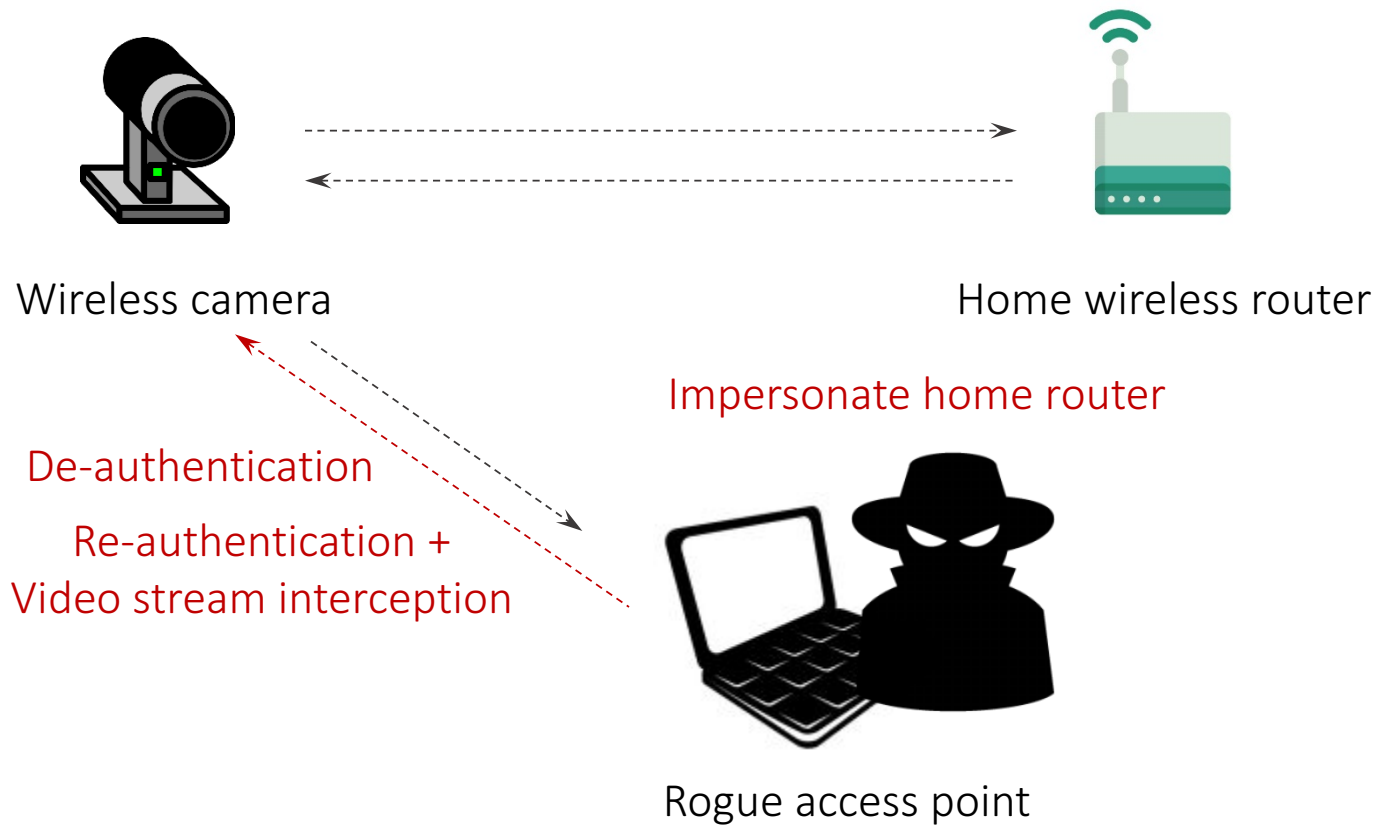
A range of appliances controllable via a mobile app

Obvious benefits…

- Lower carbon footprint

- Personalisation (access control)

- Increased comfort and safety (?)

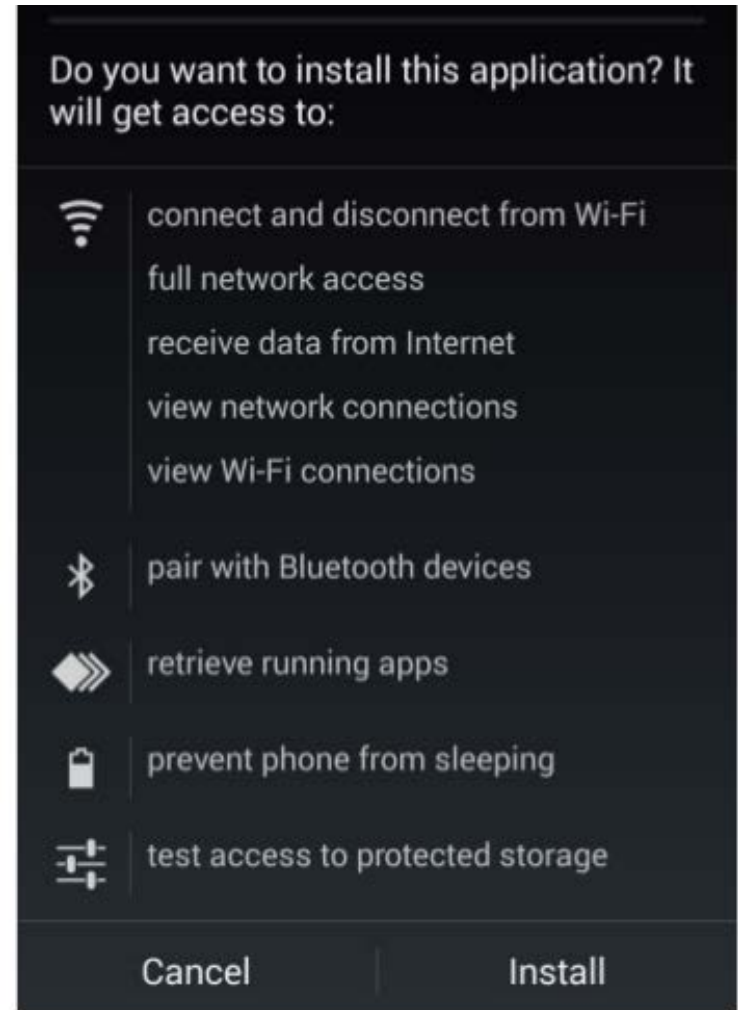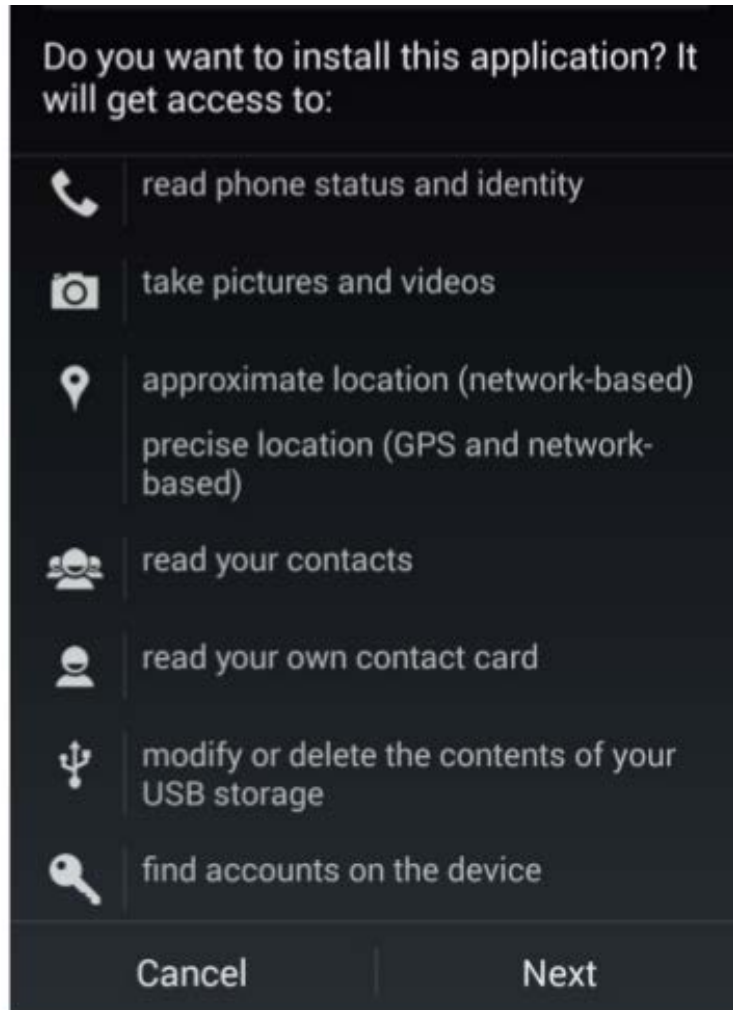# …come with risks

- Communication again wireless and subject to abuse

- Control via software (app) – risk of malware and privileges abuse

- Hijacking and weaponisation

Example: Taking down a surveillance camera

Wireless camera

Home wireless router

Impersonate home router

De-authentication

Re-authentication +
Video stream interception

Rogue access point

Example: Faking IoT device and exploiting generous app permission

Do you want to install this application? It will get access to:

📞 read phone status and identity

📷 take pictures and videos

📍 approximate location (network-based)

precise location (GPS and network-based)

👥 read your contacts

👤 read your own contact card

🔌 modify or delete the contents of your USB storage

🔑 find accounts on the device

Cancel   Next

Do you want to install this application? It will get access to:

📶 connect and disconnect from Wi-Fi

full network access

receive data from Internet

view network connections

view Wi-Fi connections

✳ pair with Bluetooth devices

⏩ retrieve running apps

🔋 prevent phone from sleeping

🎚 test access to protected storage

Cancel   Install

Example: Faking IoT device and exploiting generous app permission

Android Phone   Fake WeMo Device

"Find connected devices"

UPnP broadcast over UDP
M-SEARCH for urn:Belkin:device:** → Phone searches for WeMo devices

HTTP over UDP
http://<ip>:49153/setup.xml ← WeMo responds with its URL

HTTP over TCP
GET /setup.xml → Phone requests device description

HTTP response ← WeMo returns device description

- Possible to ask phone app to send photos taken by user, list of contacts, and other sensitive information

What we can do

Help design systems with scalability in mind.

Work to achieve strong encryption with limited computing capabilities.

Standardise security by design.

Define sustainable development of new devices.

Train developers/engineers that understand embedded systems, programming, and security.