Security, Privacy, Ethics and Sheep

Professor Stephen Hailes

UCL

UCL

UCL

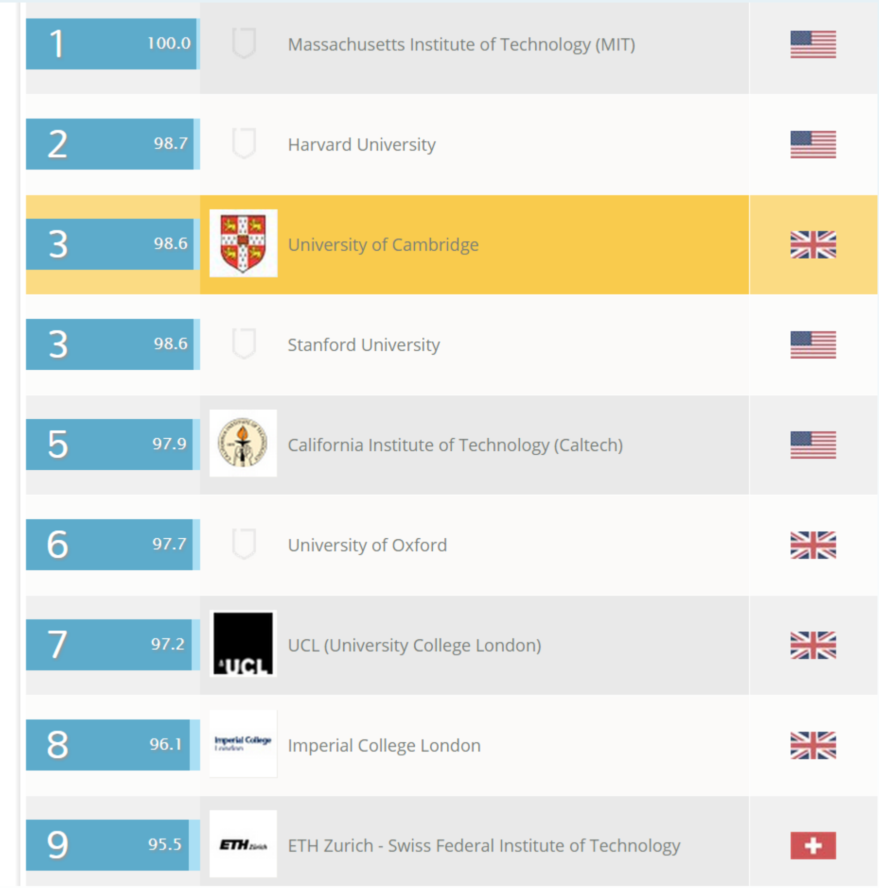
- ❑ Founded in 1826 as a University for all - inspired by Jeremy Bentham
- ❑ Establishing a radical, pioneering tradition in higher education
  - ❑ First to admit students regardless of gender, race or religion
  - ❑ First to have professors in law, medicine, architecture, chemistry, English, German, Italian, geography, French, zoology, Egyptology, and electrical engineering
  - ❑ 29 Nobel Laureates
    - ❑ Sir Charles Kao – the father of fibre optics
  - ❑ Sir John Ambrose Fleming
- ❑ ~36,000 students from 150 countries

UCL stats

Income 2013-14	
Research grants and contracts	£427.5m
Academic fees and support grants	£364.2m
Funding council grants	£187.4m
Other operating income	£194.5m
Endowment income and interest receivable	£6.1m
Total	**£1,179.7m**

Staff	
UCL Arts & Humanities	180.9
UCL Brain Sciences	856.6
UCL Built Environment	215.6
UCL Engineering Sciences	**503.0**
UCL Laws	64.5
UCL Life Sciences	529.0
UCL Mathematical & Physical Sciences	595.8
UCL Medical Sciences	699.2
UCL Population Health Sciences	820.0
UCL School of Slavonic & East European Studies	46.7
UCL Social & Historical Sciences	348.2
FTE total (October 2014)	**4,859.5**

QS world rankings…



1	100.0	Massachusetts Institute of Technology (MIT)
2	98.7	Harvard University
3	98.6	University of Cambridge
3	98.6	Stanford University
5	97.9	California Institute of Technology (Caltech)
6	97.7	University of Oxford
7	97.2	UCL (University College London)
8	96.1	Imperial College London
9	95.5	ETH Zurich - Swiss Federal Institute of Technology

~36,000 students 2014-15
(~16,000 UG; ~19,000 PG)
From 150 countries

UCL East

11 acres: 125,000m^2 of space, with the first major construction phase of the development establishing an operational presence on the Park by autumn 2018. First phase ~50,000m^2

Department of Computer Science

- ❑ Internationally leading centre of computing research
- ❑ REF2014: Top UK university in CS
- ❑ And teaching:
  - ❑ Strong relationships with Microsoft, Google, banks, gaming industry, …
- ❑ Strong emphasis on *experimental computer science*
- ❑ ~76 academic + teaching staff
- ❑ ~160 PhD students

Me:

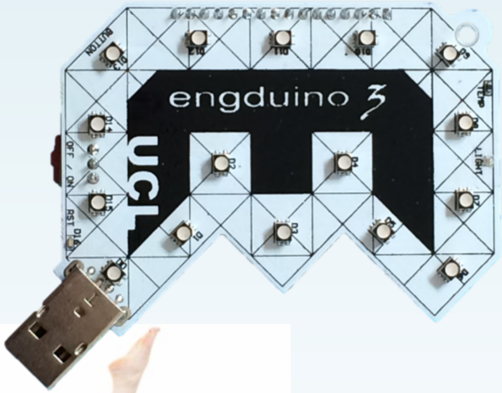
- ❑ MA & PhD in Computer Science
- ❑ Started as an RA at UCL, working on networked multimedia
- ❑ Lecturer, research moved to mobile and sensor systems

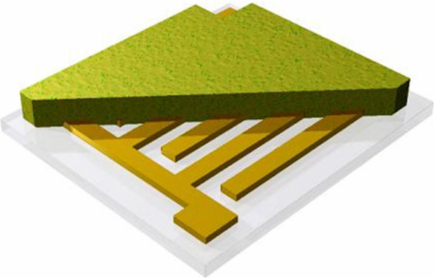
- ❑ Deputy HoD, Professor of Wireless Systems, Head of Autonomous Systems.
- ❑ Visiting professor, Royal Veterinary College

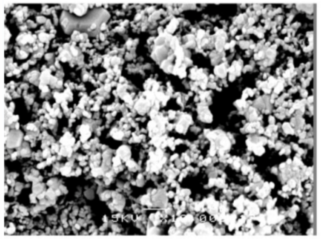
- ❑ Current research is interdisciplinary:
  - ❑ Sensors: biology, chemistry, earth science, medicine, rehab, childhood behaviour
  - ❑ Control systems, robots, localisation, security, the IoT
  - ❑ Education
- ❑ We design sensors, build hardware, gather data, do new maths, do new science, build robots, ….

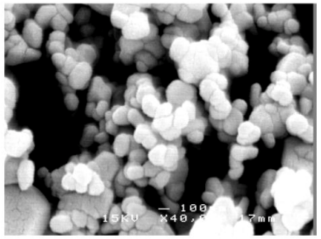
Animals

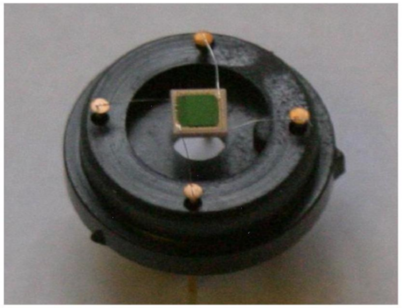
And other stuff











IOT

IoT

- IoT is coming – technologies to allow it to happen exist and are constantly reducing in price
  - wireless SoC ~ CC2538 is $5.29 in quantities of 2000
  - CISCO and others have identified markets with potential value of $trillions
- IoT has many properties, one of which is likely to be the longevity of attached devices. Another is (stable) networked control.

- Much of what takes to make it a commercial success can be represented as challenges that lie in:
  - **Engineering** – designing and building robust, secure, and extensible systems, and managing and adapting them over time
  - **Social acceptance** – gaining (or at least not abusing) the trust of end users – implies consideration of privacy and the perception of control
  - **Research** – much of which is in data processing, filtering, fusion, aggregation, modelling and presentation, and in control.
  - **Mixtures of the above** – issues like power saving for battery powered devices, localisation, and security/privacy are cross cutting

Net Result

- ❑ More intelligent sensing and control systems
- ❑ Greater connectivity
  - ❑ …giving greater availability of data and control
  - ❑ …which enables qualitatively different commercial opportunities
  - ❑ [Potentially] HUGE impact on society
  - ❑ BUT… scale and granularity of adoption → impact of system failure significant (people may die)
  - ❑ UIs will not be getting significantly better
  - ❑ Heterogeneity, adaptability, limited device capabilities and lack of clarity in management make it harder to ensure network availability
- ❑ Invisibility, heterogeneity → complex → autonomic response needed
  - ❑ No global management infrastructure, perimeter model not valid
  - ❑ Want systems to be self-configuring, adapting to context change
  - ❑ Need to understand trust (many levels) and to worry about privacy

…cont

- ❑ Assessing whether a (set of) fault(s) results from DoS is hard if node ‘failure’ rate high.
  - ❑ c.f. sensor nets for harsh environments
- ❑ Asymmetry between capabilities of attacker and attackee
- ❑ IDS related to DoS – what’s normal?

Case studies

- Monitoring children for signs of autism (w. Cambridge)
- Monitoring children for JIA (ICH/GOSH)
- Monitoring wheelchair users (ARG)
- Monitoring the elderly – dementia patients (DRC)

- Medical records & devices – held to a different standard
  - Or so you might think…
- Is anonymisation enough?
- How do we do it?
  - E.g. location privacy

UCL

Arthritis Research UK | centre for adolescent rheumatology

Juvenile Idiopathic Arthritis

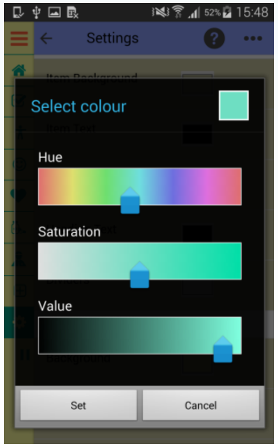
❑ < 16 years of age

❑ 1 in 1,000 children in the UK

❑ Symptoms

❑ Mobile app

❑ + sensors



15:48

Settings

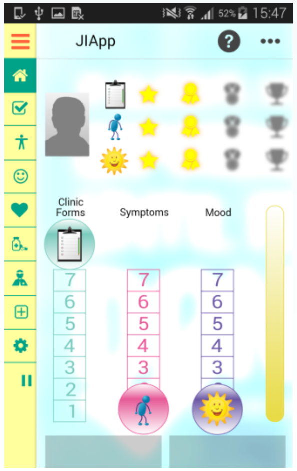
Select colour

Hue

Saturation

Value

Set | Cancel



15:47

JIApp

Clinic Forms | Symptoms | Mood

- HAQ
- Symptoms
- Mood

Arthritis Research UK
Providing answers today and tomorrow

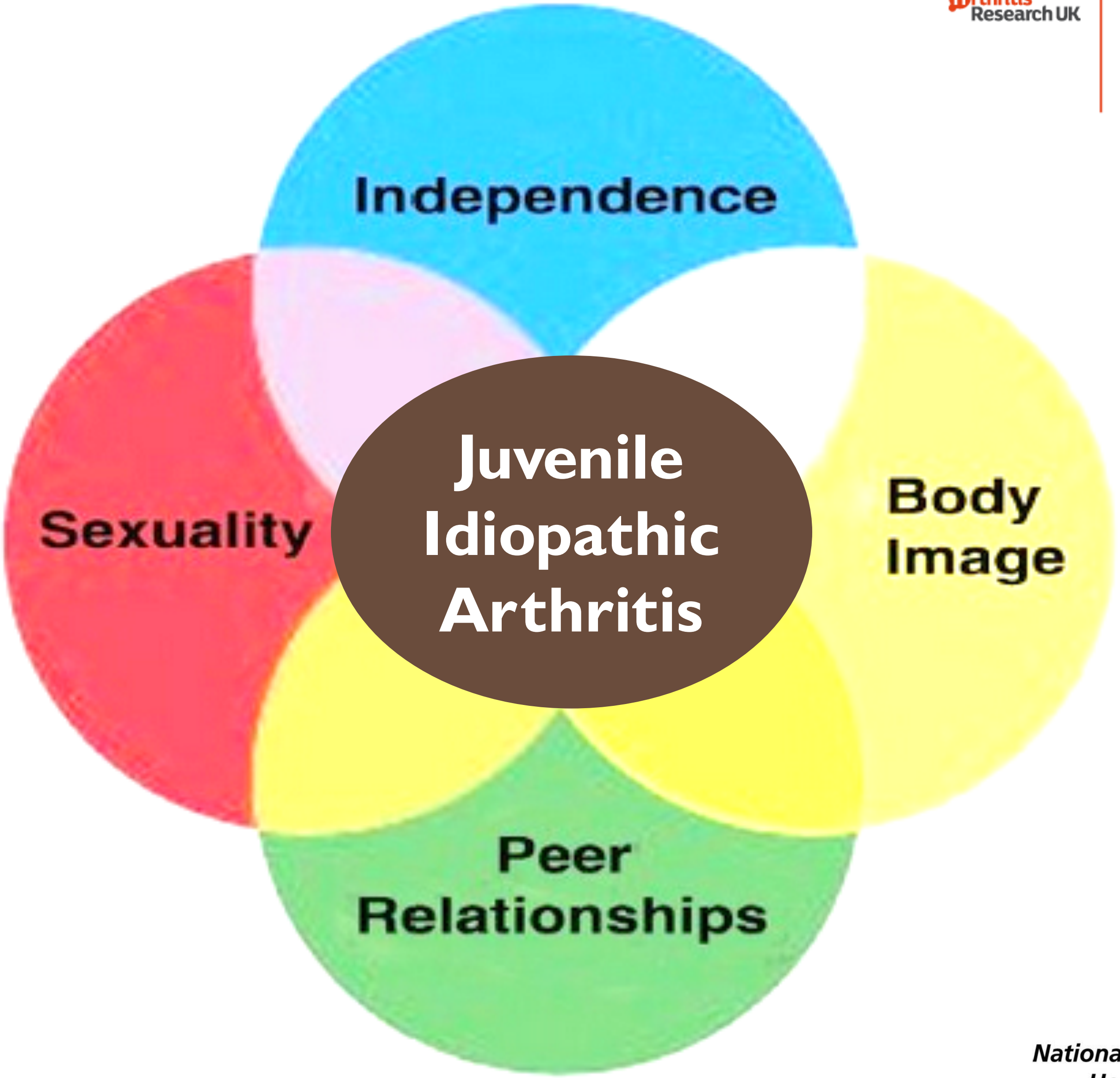
University College London Hospitals NHS
NHS Foundation Trust

Great Ormond Street Hospital for Children NHS
NHS Trust

NHS
National Institute for Health Research

UCLPartners
Academic Health Science Partnership

Great Ormond Street Hospital Charity



Arthritis Research UK | centre for adolescent rheumatology

Arthritis Research UK
Providing answers today and tomorrow

University College London Hospitals NHS
NHS Foundation Trust

Great Ormond Street Hospital for Children NHS
NHS Trust

NHS
National Institute for Health Research

UCLPartners
Academic Health Science Partnership

Great Ormond Street Hospital Charity

Security and Privacy

- ❑ Are security and privacy different?
- ❑ Generally – privacy implies a need for security, but not vice versa.

SECURITY

OK, so what is security?

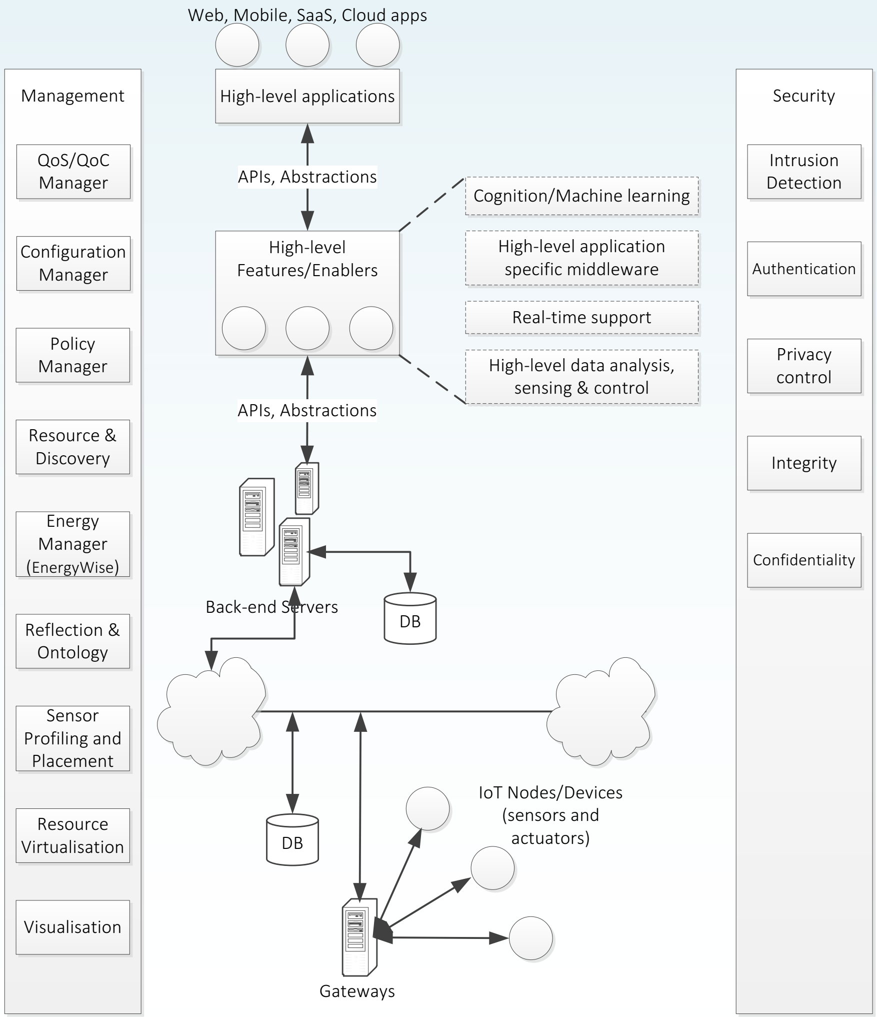
- ❑ Computer security is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.

  It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures. **Wikipedia.**

- ❑ Security is about securing a **system**
- ❑ Security is a **process** NOT a product
- ❑ A sole focus on technology is blinkered and founded in ignorance. A little knowledge is a dangerous thing
- ❑ If you think encryption is the sole answer to the question of security, you probably asked the wrong question.

Elements of IoT deployments

- ❑ End nodes/Devices/Things (including sensors and actuators),
- ❑ Database(s),
- ❑ Auxiliary computing nodes and/or servers,
- ❑ Software elements (features like profiler, configurator, machine learning, attack detection) ,
- ❑ Policies or rules (e.g., high-level management requirements or security constraints),
- ❑ Applications (specific instances or software packages engineered for a given purpose),
- ❑ Network(s) (including gateways/routers, protocols),



Why is there a security problem?

- ❑ Loads of money + intellectual property (=money)
- ❑ Hostile environment (motivations for attack vary)
- ❑ Lack of security consciousness
- ❑ Lots of potential points of attack
- ❑ Policies are often seen as unacceptable
- ❑ No regulatory framework
- ❑ Legal aspects unclear
- ❑ Restrictive export rules (?)

Security

- ❑ What changes in the IoT:
  - ❑ Resource poverty: relatively low processing power and energy stores
  - ❑ Asynchrony: your devices are switched off most of the time
  - ❑ Clock sync is not a given and is important
  - ❑ Mobility, the importance of location
  - ❑ Poor access to the hardware
  - ❑ Byzantine is the norm – things fail, but frequently not cleanly.
  - ❑ Cascading failure is the norm
  - ❑ Boundaryless security
    - ❑ Self protection
    - ❑ Intrusion detection
    - ❑ Many more points for information leakage
  - ❑ New DoS attacks
    - ❑ e.g. sleep deprivation
  - ❑ Actuators

…cont

- ❑ Security management
  - ❑ Policy
  - ❑ SW update
  - ❑ Who to tell? And in what way?
- ❑ Privacy
  - ❑ Whose data/information is it anyway? Can I opt out? When?
  - ❑ Associating information leakage with breach
- ❑ In Industrial Control Systems
  - ❑ Legacy Systems, COTS systems
  - ❑ Threats poorly understood
  - ❑ Risks very substantial
  - ❑ Almost no crossover in expertise between security engineers and control engineers

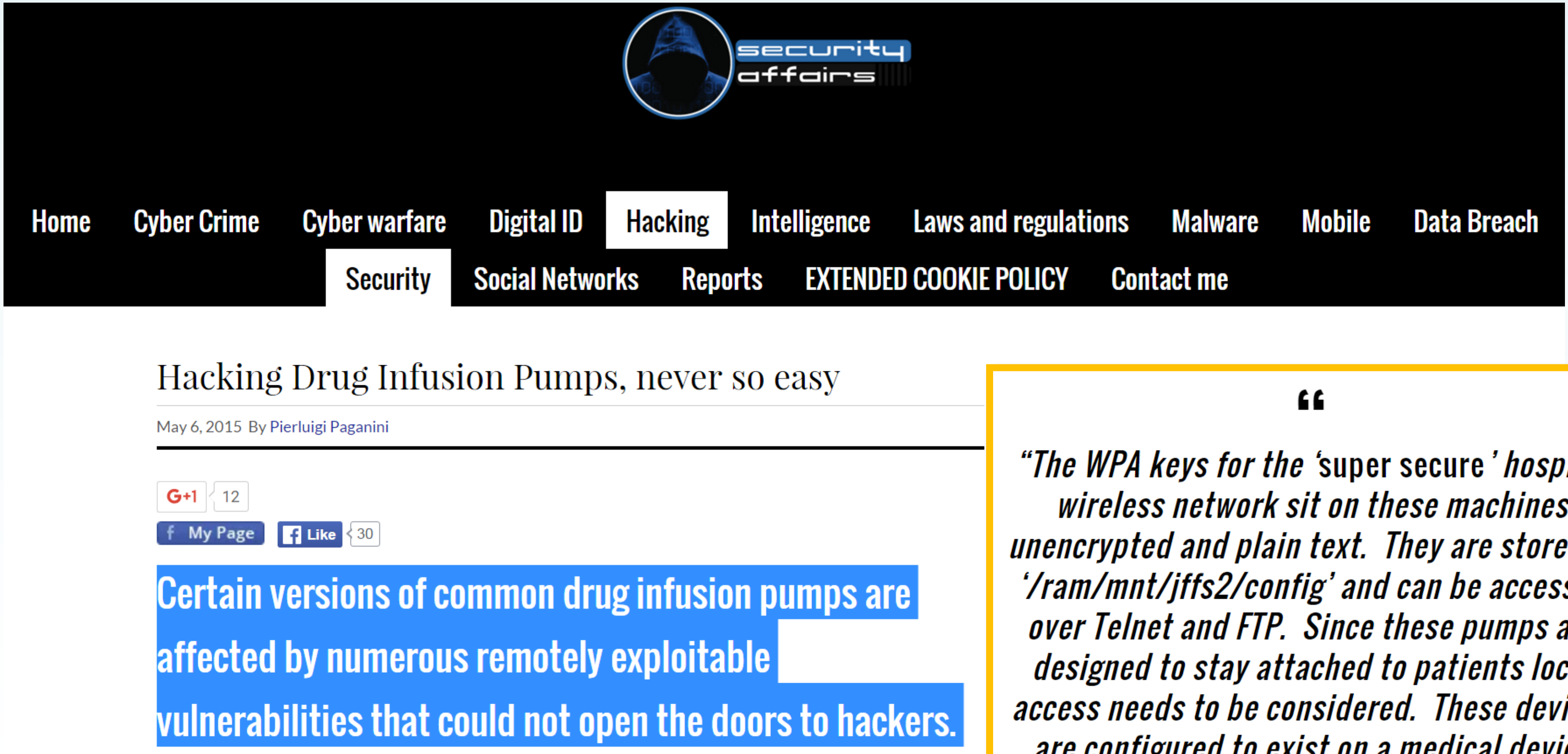
So how do we build a secure system?

- ❑ ISO 27000 series (e.g. ISO 27001:2005 – :2013 different)
- ❑ **Plan (establishing the ISMS)**
  - ❑ Establish the policy, the ISMS objectives, processes and procedures related to risk management and the improvement of information security to provide results in line with the global policies and objectives of the organization.
- ❑ **Do (implementing and workings of the ISMS)**
  - ❑ Implement and exploit the ISMS policy, controls, processes and procedures.
- ❑ **Check (monitoring and review of the ISMS)**
  - ❑ Assess and, if applicable, measure the performances of the processes against the policy, objectives and practical experience and report results to management for review.
- ❑ **Act (update and improvement of the ISMS)**
  - ❑ Undertake corrective and preventive actions, on the basis of the results of the ISMS internal audit and management review, or other relevant information to continually improve the said system.

Challenges

- □ Trust/key establishment
- □ Secure community management
- □ Privacy
- □ Policy specification (from formal languages to HCI aspects to management)
- □ Power awareness
- □ Integrity
- □ Assurance of middleware/components
- □ Secure control loops
- □ Perimeter devices in an open environment
- □ Secure routing
- □ Secure handoff (at many levels – network + service)
- □ Intrusion Detection – (who responds?, honeypots??)
- □ (For sensor nets) Secure data aggregation
- □ Monitoring of neighbouring devices
- □ New worms/viruses/spam(?)
- □ Feature interaction
- □ Standardisation: interoperable solutions
- □ Education

This is real….



Hacking Drug Infusion Pumps, never so easy

May 6, 2015 By Pierluigi Paganini

Certain versions of common drug infusion pumps are affected by numerous remotely exploitable vulnerabilities that could not open the doors to hackers.

> *“The WPA keys for the ‘super secure’ hospital wireless network sit on these machines unencrypted and plain text. They are stored in ‘/ram/mnt/jffs2/config’ and can be accessed over Telnet and FTP. Since these pumps are designed to stay attached to patients local access needs to be considered. These devices are configured to exist on a medical device network. This also needs to be considered by hospitals selling their old equipment.” Richards added.*

PRIVACY

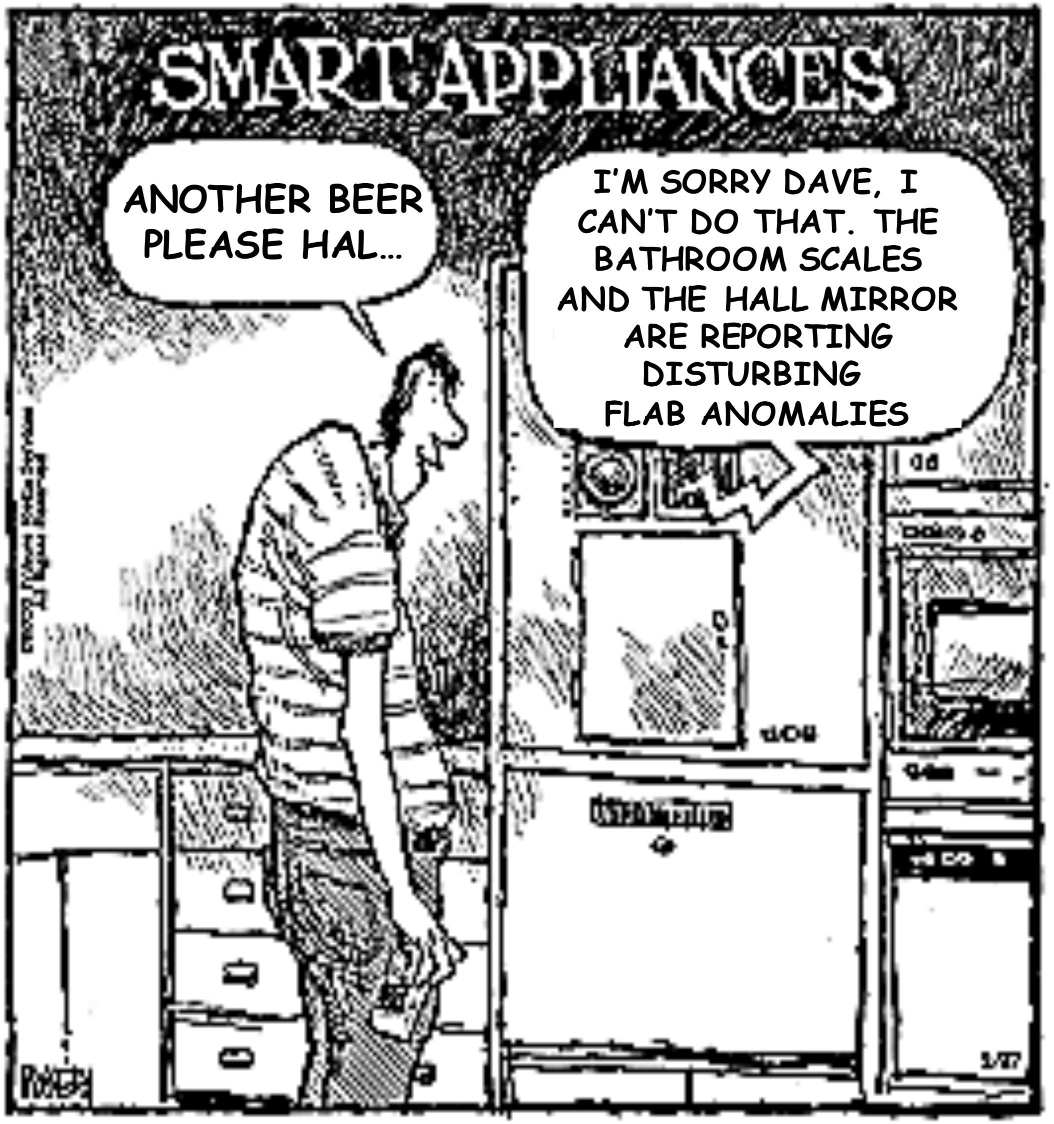
Sensors and actuators (transducers)

□ Thermal
□ Electromagnetic
□ Mechanical
□ Chemical
□ Optical and radiation
□ Ionising radiation
□ Non-ionising radiation
□ Acoustic
□ Motion
□ Orientation
□ Distance

□ Software status

□ Electrical motors
□ Pneumatic actuators
□ Hydraulic pistons
□ Relays
□ Piezoelectric actuators
□ Electroactive polymers

□ Software update


SMART APPLIANCES
ANOTHER BEER PLEASE HAL...
I'M SORRY DAVE, I CAN'T DO THAT. THE BATHROOM SCALES AND THE HALL MIRROR ARE REPORTING DISTURBING FLAB ANOMALIES

Good

- ❑ Potential to do good is substantial:
    - ❑ Health:
        - ❑ 25 million people will die of coronary heart conditions by 2025.
    - ❑ Aging population:
        - ❑ The worldwide population over 65 will be 761 million by 2025
        - ❑ 50% increase in expected lifespan in the last 50 years
        - ❑ opportunity to enable people to stay within their home environments using embedded technology.
    - ❑ Cars and buildings:
        - ❑ It is already the case that networked embedded systems are being deployed within cars and buildings (CANbus, CANopen, etc).
    - ❑ Environmental monitoring/disaster response.
        - ❑ Disasters affecting millions of people: various earthquakes, the Tsunami, and Hurricane Katrina
        - ❑ Effective prediction and response are likely to be key factors in a world in which climatic changes are likely to mean the greater frequency in extreme conditions.

Social, political, ethical issues

❑ Socially, this is a **really** important innovation.

❑ When people were asked, the issues regarded as most important both in terms of impact were:

- ❑ fear of loss of control
- ❑ the increased possibility for surveillance offered by IoT
- ❑ profiling and security risks
- ❑ new opportunities for crime.

- ❑ Complexity: the decision making process behind intelligent systems and the way valuable information is produced is not transparent.

Source:SWAMI

Privacy issues

- ❑ “**Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others** ” (Westin, 1967).
- ❑ Aka *informational self-determination*.

- ❑ Other concerns: “death of privacy”
  - ❑ individuals are completely transparent
    - ❑ They feel they are not in control of the technologies, but are controlled
  - ❑ power structures tend to be opaque
    - ❑ Some groups can fight a loss of control over technologies, some lack the intellectual, social or financial resources
  - ❑ increasing dependency on AmI systems
  - ❑ no public participation in AmI development process

- ❑ Informed consent

Privacy issues

- ❑ Privacy breach necessarily involves obtaining information about an individual; but we can only control access to data
  - ❑ Data mining
  - ❑ TIA

  - ❑ *"While discrete observations of an individual's idiosyncratic behavior can appear almost random, typically there are repeating and easily identifiable routines in every person's life"*

    N. Eagle and A. Pentland: *Eigenbehaviors: Identifying Structure in Routine*

    - ❑ 100 subjects at MIT, with Nokia 6600 smartphones using Context application that recorded:
      - – Call logs, Bluetooth devices in proximity, cell tower IDs, application usage, phone status
      - – 450,000 hours of data, subject to automated analysis
    - ❑ At lunchtime, predict day's remaining behaviours with 79% accuracy
    - ❑ Can predict group affiliations with 96% accuracy

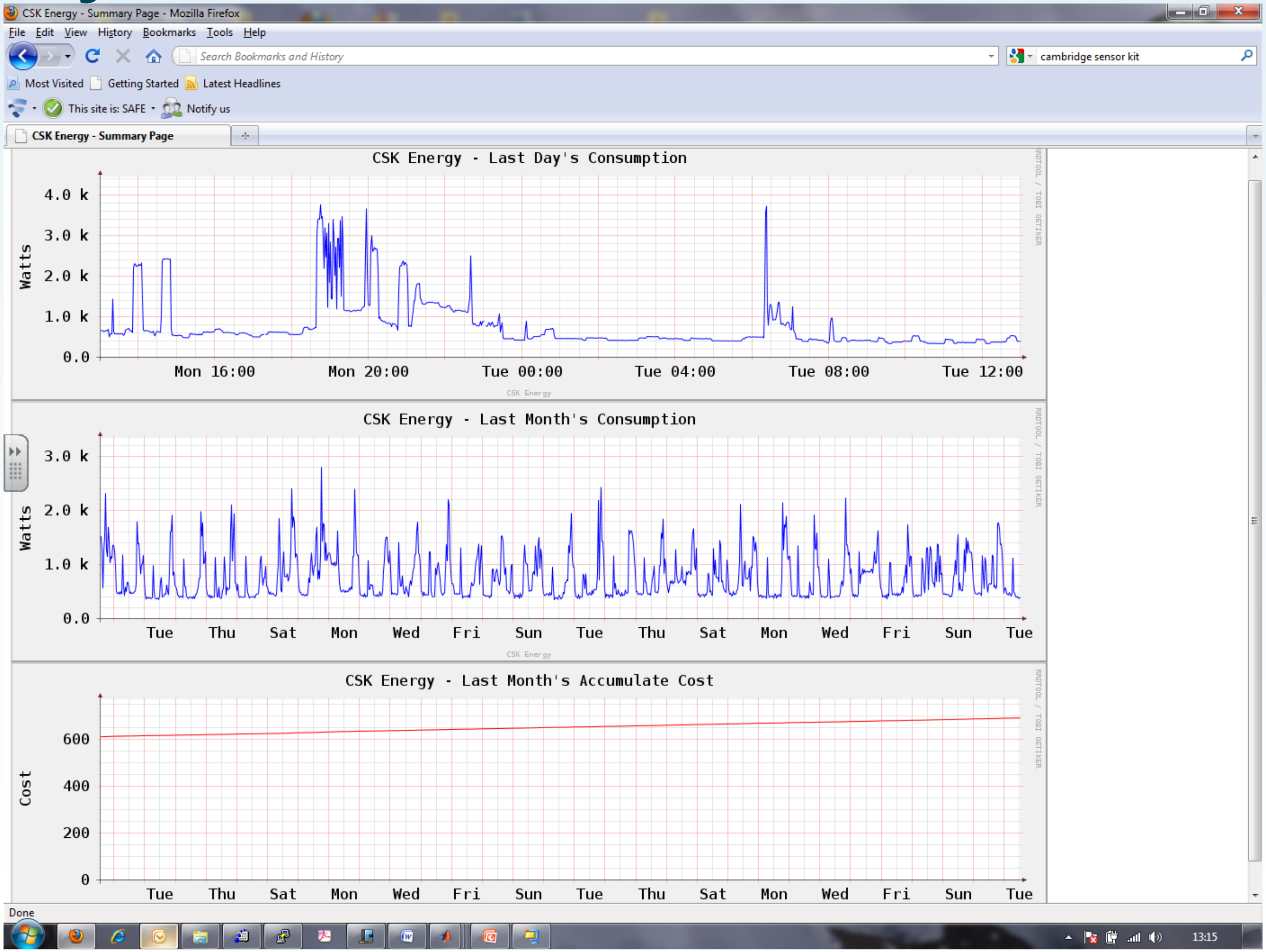
Privacy issues

- ❑ Laws to protect privacy – partly by restricting the purposes to which information can be put. But:
  - ❑ Unclear what data is being captured, let alone what information
  - ❑ There will be lots of data produced by systems under our control and those not
  - ❑ (V. complex) autonomic interaction and control implies external management and impenetrability
  - ❑ No ability to review data in a meaningful way
  - ❑ V. hard to associate a breach of privacy with actions that arise as a result of that breach – question of enforceability.

- ❑ Can we make enforceable policy in this area?

- ❑ Can we really have informed consent?

Privacy?


CSK Energy - Summary Page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Search Bookmarks and History
cambridge sensor kit
Most Visited
Getting Started
Latest Headlines
This site is: SAFE
Notify us
CSK Energy - Summary Page
CSK Energy - Last Day's Consumption
Watts
4.0 k
3.0 k
2.0 k
1.0 k
0.0
Mon 16:00
Mon 20:00
Tue 00:00
Tue 04:00
Tue 08:00
Tue 12:00
CSK Energy
CSK Energy - Last Month's Consumption
Watts
3.0 k
2.0 k
1.0 k
0.0
Tue Thu Sat Mon Wed Fri Sun Tue Thu Sat Mon Wed Fri Sun Tue
CSK Energy
CSK Energy - Last Month's Accumulate Cost
Cost
600
400
200
0
Tue Thu Sat Mon Wed Fri Sun Tue Thu Sat Mon Wed Fri Sun Tue
Done
13:15

A quotation (probably)…

“Privacy is dead, deal with it”

Scott McNealy, Chairman and CEO of Sun Microsystems.

And there’s more...

With thanks to…

- ❑ Rae Harbird
- ❑ Nilufer Tuptuk
- ❑ Behzad Heravi
- ❑ Jagun Kwon