The Internet of Things: Are we running quickly into the darkness?

George Weir

george.weir@strath.ac.uk
Summary

• The Internet of Things: Are we running quickly into the darkness?
  • Yes

• Should we be worried?
  • Yes

• Can we mitigate the risks?
  • Yes (partly)
The Internet of Things is the network of physical devices, vehicles, buildings and so on embedded with electronics, software, sensors and network connectivity that enable these objects to collect and transmit data via the Internet.

This year, 2016, we will have **4.9 billion** connected things, so get ready, the Internet of Things is here to stay.

ATMs were some of the **first** Internet of Things objects as far back as **1974**.

The "Internet of Things" is a phrase that **87%** of people haven't heard of.

Back in **2008**, there were already more objects connected to the Internet than people.

Companies like **Google** and **Samsung** are investing in home devices and having a connected kitchen could save the food and beverage industry as much as **15%** annually.

The global wearable device market has grown **223%** in **2015**.

According to some estimates, the Internet of Things will add **USD 10-15 trillion** to global GDP in the next **20 years**.

By **2020**, **250 K** vehicles will be connected to the Internet.

Google's self-driving cars average about **10 000 autonomous miles** per week.

Based on "13 Internet of Things Facts Everyone Should Read" by Bernard Mee.
A natural progression?

INTERNET OF THINGS
Internet Evolution

[Diagram showing the evolution of the Internet, from Internet of Documents to Internet of Things]
IoT and Cloud

- Cloud is seen as an enabling technology
HealthSuite IoT Architecture based on AWS

Internet of things
Data sources
Connected devices
Sensor data

HSDP Home Gateway

Amazon services used by Philips are a.o.:
EC2, S3, Glacier, Lambda, SNS

prnewswire.com
Are we Running?

• Apparently, everyone is engaging with Cloud-based IoT:
INTERNET OF THINGS LANDSCAPE

Platforms & Enablement (Horizontals)
- IFTTT
- Symply
- iobridge
- ThingWorx
- SmartThings
- NINJABLOCKS
- ZEN
- Twine
- OSITO
- zonoff
- FreedomPop
- MESH SYSTEMS
- Enabling Networks
- IBM
- LG
- Cisco
- Honeywell

Applications (Verticals)

Quantified Self
- Wearable Computing
  - Pebble
  - Fitbit
  - Jawbone
  - Basis
  - Lumo

Lifestyle
- Health
  - HAPfork
  - Wahoo
  - NuMatox

- Fitness
  - Withings
  - fitbit

- Pets
  - amigo

- Toys
  - sifteo

- Music
  - MiTTATIONS

- Gardening
  - plantlink

- Home Improvement
  - Radiator Labs

- New Interfaces
  - gestigon

Connected Home
- Home Automation
  - SmartThings
  - NINJABLOCKS
  - revolv
  -商圈
  - lapka
  - milo

- Energy Efficiency
  - knut

- Security
  - Locktron

- Smart Building
  - iSmartAlarm

Industries
- Retail
  - Nomi

- Healthcare
  - AdhereTech
  - AliveCor
  - intelligentM

- Automotive
  - Visi Mobile

- Transportation
  - TELCARE

- Aerospace
  - TELCARE

- Retail
  - Placemat

- Manufacturing
  - M2M

Building Blocks
- Connection Protocols
  - WiFi
  - Bluetooth
  - Zigbee
  - NFC
  - RFID

- Software
  - Amazon Web Services
  - iOS
  - Android

- Hardware
  - Arduino
  - Spark

- Parts / Kits
  - Adafruit

- Services
  - Kickstarter
  - Indiegogo

- Incubations
  - TechStars

- Funding
  - FirstMark Capital

© Matt Turck (@mattturck), Sutian Dong (@sutiandong) & FirstMark Capital (@firstmarkcap)
Projected Internet of Things services spending worldwide from 2014 to 2017 (in billion U.S. dollars)

Statista 2018
Third-party Internet of Things platform connectivity revenue worldwide from 2015 to 2021 (in million euros)

Third-party connectivity platform revenue is forecast to reach 1.1 billion euros in 2021.
Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)
Media prediction

• “A typical home will soon contain a network of gadgets designed to make life easier.”
  (Sunday Times, 11.01.15)
Government initiative?

The Internet of Things: making the most of the Second Digital Revolution

A report by the UK Government Chief Scientific Adviser

George Weir, 2018
Large-scale Ecosystem

Report perspective: we should engage quickly with these developments for the welfare of the population and the economic benefit of the country.
Key ingredients

• Communication
  • Wireless technology
    • Wlan
    • Bluetooth
    • GPRS (GSM)
    • New communication standards

• Integration
  • Local systems talking together and to ‘upper level’ systems

• Data analysis
  • Widely distributed data gathering
  • Centralised synthesis and analysis
Likely applications

• Home automation
  • Building management systems

• Energy
  • Smart meters

• Healthcare
  • Telehealth: delivery of remote health-related services

• Transport
  • Self-adjusting vehicles

• Agriculture
  • Sensor-based yield management
Example devices

- Smart thermostat with remote control
Apps on Your Fridge?

• ‘Upgrade your life with a Wi-Fi enabled refrigerator
• Featuring a brilliant 8” touchscreen that puts access to apps at your fingertips
• Check the morning weather, browse the web for recipes, explore your social networks or leave notes for your family—all from the refrigerator door’

Samsung advert
Smart toothbrush

- Bluetooth smartphone interaction
- No internet connection (yet!)
**Smart energy meters**

- Consumers with smart meters can have an in-home display (IHD) that lets them see how much energy they are using and what it will cost.
- This will let them have more control over their energy use and help them save energy and money.
How smart meters work

• Smart meters take accurate readings of your energy
• Readings are automatically sent to the supplier using wireless technology
• You can view usage online with an in-house display
• You receive an accurate energy bill without having to submit meter readings
Wearable technology

- Smart watches with sensors
  - Health and fitness applications
- Smart clothing is predicted to overtake the sale of fitness trackers by 2017

The Polo Tech smart shirt by Ralph Lauren, can measure heart rate and respiration connecting to a smartphone via Bluetooth
Wearable technology (2)

- The Polo Tech smart shirt by Ralph Lauren
- Can measure heart rate and respiration, distance travelled and calories burned
- Connects to smartphone or tablet via Bluetooth
Projected global market for autonomous driving sensor components from 2015 to 2030 (in billion U.S. dollars)
Intelligent Transport System Corridor

- Cooperative ITS Corridor
- EU project to manage cars from Rotterdam via Munich, Frankfurt, and on to Vienna
  - warning drivers of upcoming roadwork and other obstacles
  - aims to harmonize smart-road standards among different countries
Cooperative ITS Corridor

• Cameras every 100 metres
• Wi-Fi antennas every 500 metres
  • Short-range ‘car to road’ communication
• Measuring exact position of vehicles 10 times per second
  • within 1 metre accuracy
• Improved flow management
  • claims to address the ‘braking shockwave’ problem
Cars Will Talk, Then Collaborate

• Initial stage is ‘car to roadside’ communication
• Later stage extends this to ‘car to car’
Where we are

• Green wave system implemented in Glasgow City Centre (~2010)
  • Allows emergency vehicles to receive green waves to allow for safe and speedy journeys across the city
  • Vehicles tracked using GPRS transmission

• Bus stops showing expected arrivals
Health applications

- Mainly monitoring and data capture
- Some remote access to consultations
Ecosystem requirements

• Varieties of device
• Networking models
• Communication models
IoT Device Taxonomy

- **Large**
  - POS terminal, ATM, MRI
  - x86, PC-like, apps
  - Embedded Industry 8.1, Standard

- **Mobile**
  - Industry handheld, POS tablet
  - ARM and x86, shell experience, apps
  - Embedded Handheld 8.1

- **Small**
  - Gateways, wearables, panels, cars
  - ARM and x86, diverse hardware, no shell
  - Embedded Compact, Auto

- **Micro**
  - Controllers, fixed-use, sensors, actuators
  - ARM, constrained hardware, headless
  - .NET Micro Framework
Varieties of device

• Three varieties of ‘device’
  • Inert (with location markers)
  • Data gathering and relay
    • Sensor-based with data transfer
  • Decision making
    • Action based upon detected conditions
networking models

• Two networking models
  • Mobile device to local network
    • As we have presently
  • Close proximity, ad hoc networking
    • Device to device
    • Peer to peer

• These models will interact
Communication models

• Three communication models
  • Blackboard (e.g., cloud-based)
  • Client-server
  • Peer to peer
Home ecosystem

- Devices register presence and status with central management system
- Domestic sensor network
  - tracks and monitors internal systems, devices and other ‘objects’
    - including people
- Extended to ‘inert’ objects
  - e.g. through RFID tags
    - no more lost items
Home ecosystem (2)

• Domestic objects outside the home can also be tracked/monitored
  • Children
  • Pets
  • Vehicles
  • Mobile phones, ...

• Smart inventory, commercial and domestic

• Regulated service reports
  • Ease of data production for insurance
  • Home reports when selling property
Where we might be

- Highly integrated monitoring and control
  - domestic, district, regional and national

- Device self-monitoring for fault tolerance and timely repair
  - e.g., engine status monitor

- Environment monitoring for smart control
  - e.g., weather forecast affecting thermostat settings

- Significant cost benefits through better insight on system demand
  - e.g., cheaper health service

- Better guarantees of system performance
  - Quality of service enhancements through optimised production
We should be worried about

• Reliability/robustness
• Locus of control
• Privacy
• Integrity
• Accountability
• Security
• Digital Forensics
• Availability
Reliability and robustness

• Integrated systems could become mission or life critical
• Must have minimum failure rate
• Issue of performance and capacity
• Priority and contention management
Reliability and robustness (2)

• Multiple points of failure?
  • Individual devices
  • Communication links
  • Centralised services
Reliability and robustness (3)

• Mission critical?
Locus of control

WHEN THE “INTERNET OF THINGS” GOES TOO FAR...

HOLD IT RIGHT THERE TED, DON’T YOU REMEMBER WHAT YOUR DOCTOR TOLD YOU LAST WEEK ABOUT CUTTING OUT CARBS?
Locus of control (2)

- Who is in control?

“Bad news - the scale is threatening to cut off our access to the fridge...”
privacy

• Centralised data collection?
• The rise of ‘big data’ and data analytics
• Who owns the information?
• How can it be used?
  • Timely intervention (e.g., health care)
  • Targeted advertising
  • Product development
• Nowhere to hide?
• Tracking via our portable devices
Big Data and IoT
Buckhacker

A website created by anonymous hackers has been launched that allows anyone to search for unsecured sensitive data stored in the cloud.

Buckhacker is a tool that trawls servers at Amazon Web Services (AWS), a popular cloud computing platform.

AWS provides data storage to private firms, governments and universities, among others.

Exposed data has been found on it before, but Buckhacker makes searching for it much easier.

The name comes from the fact that AWS Simple Storage Servers (S3) are known as "buckets" - this is the part of AWS that Buckhacker accesses.

Strava

Fitness tracking app gives away location of secret US military bases

The app, made by Strava Labs, shows the movements of its app users around the world.

Kabul, Afghanistan on the Strava heat map
Integrity/Accountability

• Can you trust the results of data analysis?
• How could you verify?
• Who can be held to account?
  • Distributed responsibility means more complex accountability
security

• Internet of Insecure Things
• ‘Anything that can be hacked will be hacked’
• Shodan - the world's first search engine for Internet-connected devices
• Recent DDoS attacks employing IoT devices
• Malware (originating in China) has been found on US SCADA systems
Recognising the risks?

Only 30% of organizations say they are prepared for the security risks associated with the internet of things.

Source: Black Hat USA 2016 Survey, Tripwire
Security: risks

• Forms of attack
  • Target devices
  • Target infrastructure
  • Unauthorised access (to data or control)
  • Denial of service

• Most attacks use standard protocols to overwhelm targets
• If you are connected, you are vulnerable
Security: Internet of Insecure Things

• Recent issues with remote surveillance cameras

Hacks to turn your wireless IP surveillance cameras against you

Thousands of wireless IP cameras are vulnerable to remote attacks. At Hack in the Box security conference, researchers showed how to exploit the devices in "To Watch or Be Watched: Turning Your Surveillance Camera Against You" and released a tool to automate attacks.
Security: Unauthorised access

"I don't know how it happened, but there's an applet in the toaster and some guy in Norway keeps burning my toast."
Security: Health risks?

- Implanted networked medical devices

George Weir, 2018
Security: Health risks?

• Moving toward implanted devices
• Risk of illicit device access
The Internet of ransomware things...

HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!

ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.

20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!

I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!

THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!

30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.

WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!

YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.

EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.

IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.

I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.

SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!

MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".

I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
INTERNET OF THINGS OR INTERNET OF THREATS?
What risks does the IoT bring to your life and how do you use new connected devices wisely

USB-dongle for video streaming
Using the vulnerability in USB-dongle, the attacker could show false error messages to the user and urge them to reset their Wi-Fi network password.

Coffee maker
Coffee maker could contain a vulnerability that would expose users' Wi-Fi network credentials.

Baby monitor IP camera
Using credentials to the Wi-Fi network, a criminal could exploit multiple vulnerabilities in Baby monitors and spy on its owners.

Home security system
Contact sensors that use magnetic fields could be bypassed by a burglar with a powerful enough magnet.
Top Ten IoT Security Flaws

- Insecure Software/Firmware
- Insecure Web Interface
- Lack of Transport Encryption
- Insufficient Authentication
- Raised Privacy Concerns
- Failed to Protect Against Hackers Discovering User Identity
- Failed to Require Passwords
- Vulnerable to XSS, Weak Credentials etc.
- Use Unencrypted Network Services
- Collect Information

Source: Hewlett Packard’s Fortify on Demand, 2014
Digital forensics

• Where does the data reside?
• Who has authority to access logs or centrally stored data?
• Can we keep up with the proliferation of different devices?
Example

- A recent criminal case involving an Amazon Echo:
- In November 2015, James Bates was charged with first-degree murder of another man, who was found dead in Bates' hot tub
- Police in Arkansas seized Bates' Alexa-enabled Echo smart speaker from his home, and asked Amazon to hand over any pertinent information regarding the device's communication with Alexa
- Amazon denied the request in the absence of a valid and binding legal demand
Amazon Echo

• Forensic investigation in the context of Amazon Echo (and similar, Cloud-based systems) is complex

• According to Chung et al (2017)*, this requires “a new digital forensic approach for the Amazon Alexa ecosystem combining cloud-side and client-side forensics”

Availability: services

• How do we spread the benefits?
• We don’t all have the necessary infrastructure
  • High speed broadband
  • Domestic networks
  • Centralised monitoring and control systems
  • New era of ‘haves and have nots’?
Availability: quality of service

• Differing service options at different costs?
• Two tier health service with two access modes:
  • personal contact and on-line
• Latter will initially be cheaper option
• May evolve into more specialised service
  • e.g., advice and input from world leading medics, at a premium cost
Availability: data

• Who gets access to the data?
• At what cost?
• New scope for data brokers?
• New avenues for personalised adverts...
Availability: A new digital divide?

• Integrating old and new?
• Accommodating rich and poor?
• New education required?
Conclusion (1)

• The Internet of Things: Are we running quickly into the darkness?
  • Yes

• Should we be worried?
  • Yes

• Can we mitigate the risks?
  • Yes (partly)
Conclusion (2)

• What can we do?
Walk forward (with a flashlight)

George Weir – george.weir@strath.ac.uk