GRESHAM COLLEGE

20 MARCH 2018

THE INTERNET OF THINGS

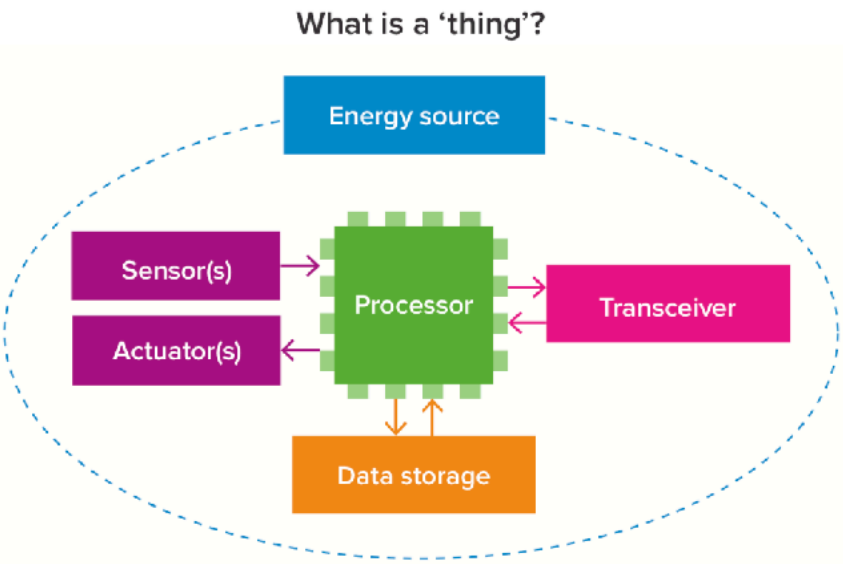
PROFESSOR MARTYN THOMAS

Introduction: The IoT – smart devices and networking

Many televisions, baby monitors, central heating systems, industrial control systems and even sex toys[i] and light-bulbs are already connected to networks such as Bluetooth, 3G or the Internet but this is only the start. Over the next few years, many billions of smart devices (the "things" of the Internet of Things or IoT) will be connected and machine-to-machine data will become the main network traffic.

The phrase "Internet of Things" was first used in 1999 by Kevin Ashton (to describe a world where most objects contained radio frequency ID (RFID) tags) and it has become increasingly common (though with no consensus on capitalisation)[ii]. By December 2014 there were already said to be more networked devices than there were people on the planet and the IoT's importance had been recognised by the UK Government; a Government Office for Science report[iii] was published in December that year. This lecture considers how the rapid growth in connected devices is likely to change our world and our lives.

Internet of Things - but what is a "Thing"?



A typical IoT device will either have a sensor (so that it can measure something) or an actuator (so that it can change something in the physical world) or both. For example:

•a wearable fitness monitor may have a sensor that measures pulse rate, and another that measures the number of steps that the wearer takes.

•a security system may have an infrared sensor to detect someone moving in a room, and a switch (actuator) that con-

trols an alarm.

- a modern car may have radar and other sensors to detect the distance from other vehicles or obstacles, and actuators that control the brakes and steering.

An IoT device must also have some way of connecting to a network (shown in the diagram above as a Transceiver) so that it can send and/or receive data - usually wirelessly.

There will be a processor that controls the actuators, sensors and transceivers, possibly some data storage (for example, so that it can collect several measurements and calculate the rate of change) and some source of energy to power all the components.

Examples of IoT Devices and Applications

The Internet of Things can sometimes seem no more than a gimmick: who really needs a kettle they can control from their iPhone[iv] or a refrigerator that calls the supermarket if you run low on milk[v]? But IoT applications range from the small and personal[vi] to the vast and national. Smaller applications include wearable electronics such as personal health monitors, children's toys, baby monitors and home automation, and there are already national scale applications, exemplified by China's *South-to-North Water Diversion Project*[vii] of three canals, each over 1,000 kilometres in length, to take water from southern rivers to the dry north of China. One of these canals, the middle route, connects the Danjiangkou reservoir to Beijing and Tianjin. Its 1,400 kilometre length contains over 100,000 IoT devices to detect and report infrastructure stress, strain, vibration, displacement, earth pressure, water leakage, flow rates, pollutants and intruders[viii].

The Internet of Things includes a very great diversity of different connected devices and their applications. Some IoT systems have been in use for many years and their benefits are well established:

- Sensors in Rolls-Royce aircraft engines stream data about the engines' usage and condition back to the manufacturer so that they can optimise maintenance; this has allowed them to change their business model to to sell engine usage rather than physical engines;
- embedded health devices such as heart pacemakers can provide early warnings of deteriorating medical conditions and can allow reprogramming without the need for invasive surgery;
- data from connected vehicles and consumer smartphones has allowed traffic flow to be monitored in real time and fed back to satnavs to provide route guidance to motorists;
- connected CCTV cameras and automated numberplate recognition allow law enforcement agencies to track vehicles in real time;
- IoT devices enable retailers to manage stock levels efficiently and to detect shoplifting;
- IoT devices enable monitoring of the environment in places ranging from deserts to the Arctic and to outer space.
- Streetlights in San Diego and elsewhere have CCTV and sensors for sound, temperature, pressure, humidity, vibration, and magnetic fields. They can monitor parking spaces, locate gunshots, report car accidents, estimate traffic density and much more[ix].

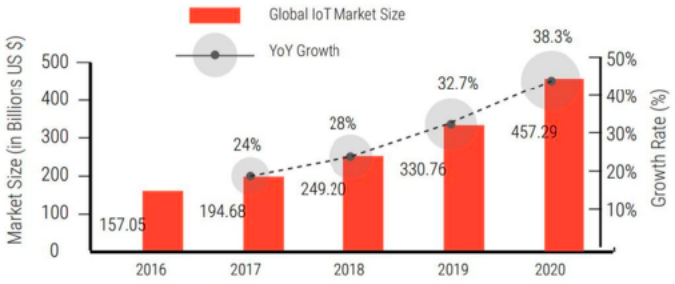
IoT applications are constantly expanding, limited only by the inventiveness of designers and engineers. A 2015 report from the Internet Society[x] grouped IoT applications by **location**[xi]:

- **Human**: devices attached to the body or inside it, such as fitness monitors, pacemakers and smart pills that can report when they have been ingested[xii] …
- **Home**: internet connected kettles, refrigerators, heating, lights, toys, locks, baby monitors, smart meters, alarms, cameras, televisions, voice assistants (e.g. Alexa ™)…
- **Shops**: self checkout, inventory control, data collection, security cameras …
- **Offices**: mobile devices, energy management, security, staff monitoring …
- **Factories**: mobile control and data entry devices, hoists, industrial control systems, security and staff monitoring …
- **Hospitals**: patient monitors, infusion pumps, syringes, thermometers, equipment location, MRI scanners, X-ray machines, environment monitoring and control, pagers …
- **Worksites**: predictive maintenance, condition monitoring, control and instrumentation, equipment location, remote control of cranes and access platforms …
- **Vehicles**: control and monitoring of cars, vans, lorries, ships aircraft, condition-based maintenance, usage analysis …
- **Cities**: traffic sensing and control, metro and light rail control and monitoring, law enforcement, information and advertising displays and sensors, monitoring and control of smart buildings, energy usage optimisation, taxi and courier tracking, air quality monitoring …
- **Outside**: inter-urban and inter country navigation and real-time routing, shipment tracking, weather sensing, fisheries protection, control, monitoring and security of offshore platforms and wind farms …

Governments have welcomed the opportunities that the IoT offers for new industries, reduced costs and increased productivity and tax revenues. The large management consultancies have recognised that the IoT is another major opportunity to sell consultancy services and they have issued reports full of predictions and advice for their clients. The forecasts differ but the consensus is that the IoT will be huge and very valuable; as just one example, a 2016 report[xiii] from EY media and entertainment group quotes IoT growth figures from IDC (30 billion IoT devices and an IoT market of $1.46 trillion by 2020) and from Gartner (20.8 billion devices and $3 trillion market, also by 2020).

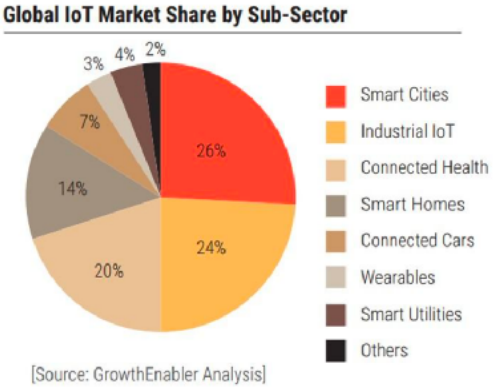
The Market Pulse report[xiv] by GrowthEnabler in April 2017 showed the forecast growth graphically, saying that the global IoT market will grow from US $157bn in 2016 to US $457bn by 2020, at a compound annual growth rate of 28.5% (data from MarketsandMarkets). The three countries competing to capture global IoT market share, by 2025 will be the USA (22%) followed by China (19%) and Japan at 6% (data from Machina Research).

The UK is said to have only 2% of global markets but the UK's share is *"expected to accelerate as investment increases"*.



[Sources: GrowthEnabler Analysis/MarketsandMarkets]

GrowthEnabler say that the three largest IoT market sectors are Smart Cities (26%), Industrial IoT (24%) and Connected Health (20%), followed by Smart Homes (14%), Connected Cars (7%), Smart Utilities (4%) and Wearables (3%).



[Source: GrowthEnabler Analysis]

Harriet Green, the Chief of IoT at IBM, is quoted as saying:

> *"It's not so much about the emergence of new technology, it's the convergence – the ability to use sensors for everything in the world to basically be a computer, whether it's your contact lens, your hospital bed or a railway track".*

Engineering Issues in the Internet of Things

The developers of IoT devices and systems face some difficult engineering challenges.

- The need to connect many billions of addressable devices soon exhausts the 32-bit address space of the Internet Protocol IPv4, as 32 bits only provides 4,294,967,296 unique addresses. The number of IP addresses available for devices to connect to the Internet has grown with the introduction of IPv6[xv] from just over 4 billion to 340 trillion, trillion, trillion (which should last as long as the planet does) but IPv6 has still not been fully adopted.
- When IoT devices are embedded in buildings, in civil engineering infrastructure, in remote or inaccessible locations (such as offshore or inside nuclear reactors) or in products with a long design lifetime then they need to be designed to survive in hostile environments and to contin-

ue to function acceptably for many years. They must be physically and electronically robust and capable of being updated securely when vulnerabilities or other defects become apparent.

- In many applications IoT devices will need to have very low power usage or even to be able to obtain sufficient power from the environment in which they are located, for example by harvesting energy from radio waves[xvi] so that they continue to function for as long as necessary – which in some applications might be several decades.

- IoT devices need networking capabilities that suit their environment, perhaps by using nearby IoT devices to relay data packets[xvii].

- If IoT devices are used in large volumes or as part of inexpensive products they need to be cheap and yet still fit for purpose and adequately secure.

- If IoT systems are handling personal data then they will need to comply with local legislation (the General Data Protection Regulation[xviii] in the EU, for example) which may impose duties to obtain informed consent from the data subject before processing their personal data, plus an obligation to deliver their data to the data subject on request, to delete it securely when requested to do so, and more. In early 2018, it is not yet clear how GDPR will be interpreted and enforced across the diversity of IoT systems and what the impact will be.

There are also problems of complexity and the unintended consequences of newly-introduced IoT devices interacting with existing IoT devices and forming unintended systems with unforeseen properties and feedback loops.

Security

The security of the Internet of Things has grown in importance since 2009 when John Matherly, a software engineer based in Texas, developed a unique search engine as a tool for market research[xix]. His idea was to be able to tell firms who was using their software and whether they had taken the latest updates but people who used it soon began to find all sorts of systems connected to the internet: printers, cameras, traffic lights, home automation, phones, carwashes, medical devices, cars and industrial control systems – even a crematorium for example. His search engine, *Shodan*[xx], has been described as "the scariest search engine on the internet"[xxi] because some of these systems are critical to an organisation's operations or to safety or privacy and many of them have only rudimentary security – or none at all, because they were designed years ago or only intended to be attached to closed local networks and not to the internet.

It should go without saying that important systems should never be connected to the internet without adequate security (such as strong passwords, a firewall, and two factor authentication) but it can happen by accident or oversight, when an engineer connects a networked laptop to a control system to carry out maintenance, or when an administrative system is connected to an industrial system for convenience such as collecting data, or as a side-effect of introducing a new phone system. It also commonly happens when companies prioritise cost and convenience without adequate analysis of the implications for safety and security.

Consumer systems often have weak security even if they are designed to be internet connected, because effective security can add cost and as few consumers give much thought to the security of networked devices when choosing and purchasing one, manufacturers have no incentive to make the investment. Insecure devices are obviously a risk to their owners – few people want to be spied on by strangers who access their webcams or security cameras, nor do they want

strangers controlling their home automation or (as happened in April 2014) grooming or abusing their children through their internet-connected dolls or other gadgets[xxii].

Insecure consumer systems are not only a threat to the owners and their families: in September 2016 the website of the security analyst Brian Krebs' was hit by a record Denial of Service attack[xxiii] in revenge for his success in securing the prosecution of some cyber-criminals. The Mirai botnet that was used in that attack had been built from 380,000 internet connected cameras, printers and DVD players that contained the Linux operating system and that had weak security – in particular, default account names and passwords for the Linux telnet service. Once infected with the Mirai malware, the IoT devices scan the internet for other devices to infect before contacting a command website to get instructions on when and where to launch an attack. The Mirai source code was subsequently released on the internet where it remains freely available[xxiv]; it has been used for other attacks and the techniques it uses have been modified for other malware.

Although Brian Krebs tracked down[xxv] the authors of Mirai and they have been arrested, charged and have pleaded guilty[xxvi], many of the IoT devices remain vulnerable because their owners are unaware of the poor security, probably could not change the default passwords even if they knew about them, and the manufacturers lack the incentive, the ability or even the legal authority to fix the problems remotely.

These sorts of security problems seem certain to get much worse as many more IoT devices are installed in millions of new locations.

Privacy

The Internet of Things inherently raises many privacy issues – even when IoT devices are operating legitimately and when they have not been hacked, spied on or infected with malware. The UK Government Office for Science report[xxvii] observes

> *Although the Internet of Things can be conceived as billions of benign devices transmitting tiny amounts of data, value will be generated from aggregating and analysing large quantities of it. There is considerable research into novel techniques to secure connected devices, networks and data individually. However, protecting whole systems will become just as important as protecting individual components. In addition, people will be an integral part of those systems.*

IoT devices already collect personal data in unprecedented quantities and the volume will grow exponentially. The new generation of small satellites stream high definition images from space and the resolution will continue to improve to the point where individuals can be identified, even by civil satellites. Small drones with high definition cameras are being sold in very large numbers, and future drones may be as small and silent as a butterfly. Many people have installed devices in their homes that capture and stream video of anyone who is inside or nearby, and that transmit every sound across the internet (for example, to do speech recognition). Many toys (and even sex toys) are internet connected and transmit activity, usage and sounds. Modern cars collect large amounts of personal data and car companies plan to make money from it[xxviii]. A fully driverless car would need to observe everything that happens around it (and probably most of what its passengers do as well). Almost everything we do can be observed by strangers; much of it already is and the amount that is increases daily. It seems unlikely that the new General Data Protection Regulation (GDPR, effective from May 2018) can be enforced except against the most serious offenders, though there will be some fun to be had by individuals demanding (as is their right) free copies of any photograph or video that has been taken of them.

The UK Information Commissioner has published a blog[xxix] recommending steps that consumers should take when buying internet connected toys and other smart devices, and a web page with more general advice[xxx] about consumer IoT devices. The German regulator has gone further, actually banning[xxxi] smart watches for children as "spying devices", because they make it possible to track children and to listen in to everything that is happening around them.

The power of big data analysis reveals secrets even when the raw data is anonymous, as I discussed in my lecture "*are you the customer or the product?*"[xxxii] in October 2016. In November 2017, the fitness tracking company Strava released a map[xxxiii] that showed over 3 trillion GPS data points from the data uploaded to its app. According the the report in the Guardian newspaper, Strava demonstrated that the new heat-map was detailed enough to see kiteboarding in Mexico, to track the route of the Camino de Santiago across northern Spain and to see the sea route of the Ironman triathlon in Kona, Hawaii. The heat-map is interactive (and great fun); you can zoom in to any area that interests you[xxxiv]. It was also detailed enough to identify military bases and even to show their internal layout and the routes that soldiers took locally when exercising[xxxv] as the picture of a base in Helmund Province, Afghanistan, (below) shows.

▲ A military base in Helmand Province, Afghanistan with route taken by joggers highlighted by Strava. Photograph: Strava Heatmap

When even military secrets are easily revealed by the Internet of Things, it is not unreasonable to ask whether personal privacy has already been destroyed or, if some privacy still remains for now, whether it can survive.

Reporter Kashmir Hill has written[xxxvi] that

> *In December [2017], I converted my one-bedroom apartment in San Francisco into a "smart home." I connected as many of my appliances and belongings as I could to the internet: an Amazon Echo, my lights, my coffee maker, my baby monitor, my kid's toys, my vacuum, my TV, my toothbrush, a photo frame, a sex toy, and even my bed.*

She arranged for a colleague Surya Mattu to monitor what information was being collected and transmitted (within certain agreed limits). Her report is both entertaining and informative and is recommended reading for anyone considering adding more smart devices to their home.

She concluded that there were privacy issues but that her main conclusion was that living in a smart home was extremely irritating. Recently, some Amazon customers have reached the same conclusion, when their Alexa device suddenly started laughing at them[xxxvii].

Regulation

The IoT is already an important part of society and growing rapidly. Some IoT devices have life-critical functions and this role is also growing rapidly. So how is the IoT regulated? Inadequately at best - often not at all.

Harold Thimbleby and I described the inadequate regulation of medical devices in our Gresham lecture "Computer Bugs in Hospitals, A New Killer" [xxxviii]. There is nothing to stop a medical device manufacturer from releasing a product that contains critical security defects: in 2015 the U.S. Food and Drug Administration advised hospitals not to use Hospira Inc's Symbiq infusion system, saying a security vulnerability could allow cyber attackers to take remote control of the system[xxxix]. The FDA encouraged hospitals and facilities using the system to disconnect it from the hospital network, but warned that this would require manual entry of drug libraries for each pump. The FDA "strongly encouraged health care facilities to begin transitioning to alternative infusion systems as soon as possible." There have been other reports of security defects in pacemakers and many other medical devices. Former US vice president Dick Cheney had his defibrillator's wireless component disabled, fearing that a terrorist might interfere with it.

It is common that manufacturers pay insufficient attention to the quality of their software or the security of their systems when bringing new technology to market. There is high commercial pressure to win early market share, and customers will not be able to tell that a device has vulnerabilities such as off-the-shelf software components with known defects or default passwords – and even where devices are regulated, the regulators do not have the resources (or in many cases the legal powers) to make detailed checks.

In healthcare, as in most industries, there is no requirement that data should be collected about defects that are found in devices after the product has been put on the market. This means that even where products are regulated, the regulator has no data on which they could assess the effectiveness of their regulatory oversight. A 2017 research report[xl] for the European Commission (*Standardisation and Certification of the Internet of Things,* by Leverett, Clayton and Anderson) considered "what will happen to safety regulation once computers are embedded invisibly everywhere". They conclude that safety will replace privacy as the focus of security research and that much stronger regulation will be required in many industrial sectors.

In March 2018, the UK Government published a proposal[xli] that consumer IoT devices should be "secure by design", saying:

> *This report advocates a fundamental shift in approach: moving the burden away from consumers having to secure their devices and instead ensuring strong security is built into consumer "internet of things" (IoT) products by design. It also sets out the need for greater action by Government and industry, and proposes a range of measures to better protect citizens and the wider economy.*
>
> *The central proposal of this report is a draft Code of Practice aimed primarily at manufacturers of consumer IoT products and associated services. It has been developed through extensive engagement with industry and subject matter experts and sets out thirteen practical steps to improve the security of consumer IoT.*
>
> *IoT security is a global challenge requiring global collaboration. The Government is working with international partners and through international organisations to collectively take action to secure consumer IoT products and associated services at every stage of their lifecycle.*

The publication of this report, and particularly the draft Code of Practice, is intended to stimulate further dialogue with industry, international partners, academic institutions and civil society. Further details on how to provide input on the proposed interventions are included in the report.

Also being published alongside this report is a literature review which sets out a range of evidence, international activity and recommendations on the subject of IoT security.

The UK Government hopes that industry will adopt the Code of Practice voluntarily and that market forces will be enough to ensure that the IoT becomes adequately secure, though they say that they will consider regulation if necessary. Meanwhile, many insecure IoT devices will be sold and add to the millions that already exist. There is no sign yet that regulators understand the magnitude of the task that they face if they are to continue to discharge the responsibilities that society expects of them, nor is there any appetite in the UK Government to introduce regulations that might slow down innovation. Regulation and legislation are again trailing far behind developments in technology and our future society is being designed by companies that aim to maximise profits with little or no concern for the longer term problems that they introduce.

Regulation will undoubtedly be needed but the European Union is probably the only authority that may have the willingness to bring in adequate regulation and the market power to enforce it.

Conclusions

The Internet of Things is here and growing rapidly. It will affect every aspect of our lives and decisions that are taken this year will be built into products, buildings, vehicles and major infrastructure that we expect to last for many decades into the future. Will we be able to patch all the vulnerabilities that will be found, or will "consumer durables" cease to be durable and have to be scrapped when serious software or hardware defects are found? In 2028 or 2038 will anyone still be able to maintain cars built this year or next that contain a hundred million lines of software in hundreds of subsystems whose complexities are known only to suppliers that may have gone out of business? Perhaps market pressures will be enough to ensure that consumer goods are adequately safe and remain that way, but who will ensure the same for millions of medical devices, street-lamps, building management systems, security cameras, and everything else that will make up the interconnected Internet of Things in the expanding digital society? Will cybercriminals be able to use ransomware to demand "protection money" to keep each of our important systems working? Will hostile nations or terrorists exploit the growing range of ways in which they can gain power, leverage and publicity?

If our society is to remain resilient in the face of a growing threat from cybercriminals and terrorists then we shall need to invest in research, development, training and education so that digital systems are provably secure by design. The recent UK draft Code of Practice and the *Strategic Principles for Securing the Internet of Things*[xlii] from the US Department of Homeland Security are a good start but they are both insufficiently demanding and detailed. Regulation is needed, so that the risks of poor security are borne by the manufacturers and importers of insecure IoT devices and the companies that develop insecure IoT systems, because they are the only ones that can improve security and they need to have a strong incentive to do so.

We shall need to build in redundancy and to regard it as insurance rather than as inefficiency. We shall need to co-operate internationally to regulate industry so that products meet the high standards we need. All this will take investment and strategic thinking about what a safe and secure digital society will need in the decades to come.

For further reading, I recommend this report[xliii] and this one[xliv], both from the Internet Society, the report on Critical Infrastructure and the IoT[xlv] from CIGI and Chatham House, and PETRAS[xlvi], the EPSRC research hub for the IoT.

References

---

[i] https://boingboing.net/2018/02/02/sarah-jamie-lewis.html WARNING: sex toy pictures

[ii] https://books.google.com/ngrams/graph?content=internet+of+things&case_insensitive=on&year_start=1800&year_end=2008&direct_url=t4%3B%2Cinternet%20of%20things%3B%2Cc0%3B%2Cs0%3B%3BInternet%20of%20Things%3B%2Cc0%3B%3BInternet%20of%20things%3B%2Cc0%3B%3Binternet%20of%20things%3B%2Cc0

[iii] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

[iv] https://www.amazon.co.uk/iKettle-2-0-Wi-Fi-Electric-Kettle/dp/B00BHXAWX4

[v] https://www.wired.com/2014/10/is-your-refrigerator-running/

[vi] https://advocacy.mozilla.org/en-US/privacynotincluded

[vii] http://www.water-technology.net/projects/south_north/

[viii] https://spectrum.ieee.org/tech-talk/telecom/internet/a-massive-iot-sensor-network-keeps-watch-over-a-1400kilometer-canal

[ix] https://spectrum.ieee.org/computing/it/san-diego-installs-smart-streetlights-to-monitor-the-metropolis

[x] https://www.internetsociety.org/resources/doc/2015/iot-overview

[xi] Much of this classification is credited to the McKinsey Global Institute

[xii] https://newatlas.com/smart-digital-pill-fda-approval/52187/

[xiii] http://www.ey.com/Publication/vwLUAssets/ey-m-e-internet-of-things/$FILE/ey-m-e-internet-of-things.pdf

[xiv] https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf

[xv] https://www.internetsociety.org/issues/ipv6/

[xvi] https://spectrum.ieee.org/tech-talk/telecom/wireless/startup-wiliot-promises-nobattery-bluetooth-beacons-in-2019

[xvii] https://www.researchgate.net/publication/270509690_A_Survey_on_Wireless_Mesh_Network_and_its_Challenges_at_the_Transport_Layer

[xviii] https://www.eugdpr.org/

[xix] See *The Internet of Unprotected Things,* New Scientist, 14 May 2016, pp40-41.

[xx] www.shodan.io

[xxi] http://money.cnn.com/2013/04/08/technology/security/shodan/

[xxii] https://www.economist.com/news/special-report/21606420-perils-connected-devices-home-hacked-home

[xxiii] https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

[xxiv] https://github.com/jgamblin/Mirai-Source-Code/blob/6a5941be681b839eeff8e-ce1de8b245bcd5ffb02/mirai/bot/scanner.c#L123

[xxv] https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/

https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/

[xxvii] [xxvii] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

[xxviii] https://arstechnica.com/cars/2018/02/no-one-has-a-clue-whats-happening-with-their-connected-cars-data/

[xxix] https://iconewsblog.org.uk/2017/11/23/the-12-ways-that-christmas-shoppers-can-keep-children-and-data-safe-when-buying-smart-toys-and-devices/

[xxx] https://ico.org.uk/for-the-public/online/consumer-devices/

[xxxi] http://www.bbc.co.uk/news/technology-42030109

[xxxii] https://www.gresham.ac.uk/lectures-and-events/are-you-customer-or-the-product

[xxxiii] https://www.theguardian.com/lifeandstyle/the-running-blog/gallery/2017/nov/02/strava-a-global-heatmap-of-athletic-activity

[xxxiv] https://labs.strava.com/heatmap/#7.02/-3.47738/53.01510/hot/all

[xxxv] https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

[xxxvi] https://gizmodo.com/the-house-that-spied-on-me-1822429852

[xxxvii] https://www.theguardian.com/technology/2018/mar/07/amazon-alexa-random-creepy-laughter-company-fixing

[xxxviii] https://www.gresham.ac.uk/lectures-and-events/computer-bugs-in-hospitals-a-new-killer

[xxxix] https://www.reuters.com/article/us-hospira-fda-cybersecurity/fda-warns-of-security-flaw-in-hospira-infusion-pumps-idUSKCN0Q52GJ20150731

[xl] http://www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf

[xli] https://www.gov.uk/government/publications/secure-by-design

[xlii] https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

[xliii] https://www.internetsociety.org/resources/doc/2015/iot-overview

[xliv] https://www.internetsociety.org/policybriefs/iot

[xlv] https://www.cigionline.org/publications/critical-infrastructure-and-internet-things-0

[xlvi] https://www.petrashub.org/