Threat Detection

Telefónica

Trend Report

Insecurity in the Internet of Things

06/10/2015

Telefonica

Executive Summary

In terms of expectation and anticipation, the Internet of Things (IoT) is on the crest of a wave. In enterprise the IoT is seen as an integral part of the blueprint for developing from the digital business model of today to the digitisation of the entire value chain, and in the consumer space 'wearable' adoption is rising rapidly. However significant advances in edge computing, networks, big data and analytics are still required for this truly disruptive technology to shape the future; and widespread implementation is likely to be 5-10 years away.

Such scope ensures that IoT should not be thought of as just a 'Thing' in itself; it is a collection of technologies integrated and presented to provide specific and vastly diverse applications. At this nascent stage in the lifecycle, focus on securing it can be disproportionately weighted on the end device, forgetting that it is merely a component of a larger eco-system that is only as strong as its weakest link. Aside from the inherent restrictions on security measures due to size and cost of many devices, the quantity and nature of data to be collected and transmitted, and tackling user behavioural traits also provide complex challenges.

Methods to subvert these technologies will depend both on the manner in which they mature, and how security is implemented on often exposed devices. Worryingly, the early indications are that the network, application and cloud security lessons of the past 20 years have often been forgotten by existing technology vendors, and not yet learnt by manufacturers pushing into a new market.

While risk exposure from IoT vectors is likely to remain low in the short term for most enterprises, it may be higher than first thought. Some risks will undoubtedly become more relevant as the IoT ecosystem matures; fraudulent use of IoT based services, or danger of physical harm through failure or manipulation. Avoiding distraction from the future or edge cases, the uptick in reflective DDoS attacks during H2 2014 already indicates one negative consequence of an insecure IoT. The natural extension of shadow IT combined with confluence of home and office working means IoT devices may already be permeating corporate networks, and the potential of almost permissionless innovation has the potential to fundamentally change the way we look at data protection.

The concept of security by design must be given a higher priority in order to avoid security flaws being compounded as the IoT matures, and adopters should be alert to IoT integration in a less mature, loosely regulated environment, or risk costs spiralling later. Core principles of data, application, network, systems and hardware security remain applicable but the complexity is higher and measures must be more careful not to work against the user. The IoT will be transformational, disruptive technological movement, but carries a spectrum of risks that affect more than just the IT department.

Contents

The world of the Internet of Things

The International Telecommunications Union defines the Internet of Things (IoT) as the "global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies". While a nascent concept now, the scale of what this might look like even in 5 years is estimated by Cisco to number 50 billion devices [1], and has implications for advancing automation in nearly every field. However such potential brings with it much expectation; the cross industry perspective of the 2015 Gartner Hype Cycle for Emerging Technologies report [2] illustrated in Figure 1 currently places the overall concept and some of its sub-categories at the peak of inflated expectations. The timescale proposed to reach the plateau of productivity is 5-10 years, so while it may be an incoming technology tsunami, the innovators and early adopters are perhaps now more akin to the ripples far out at sea, some way from landfall.

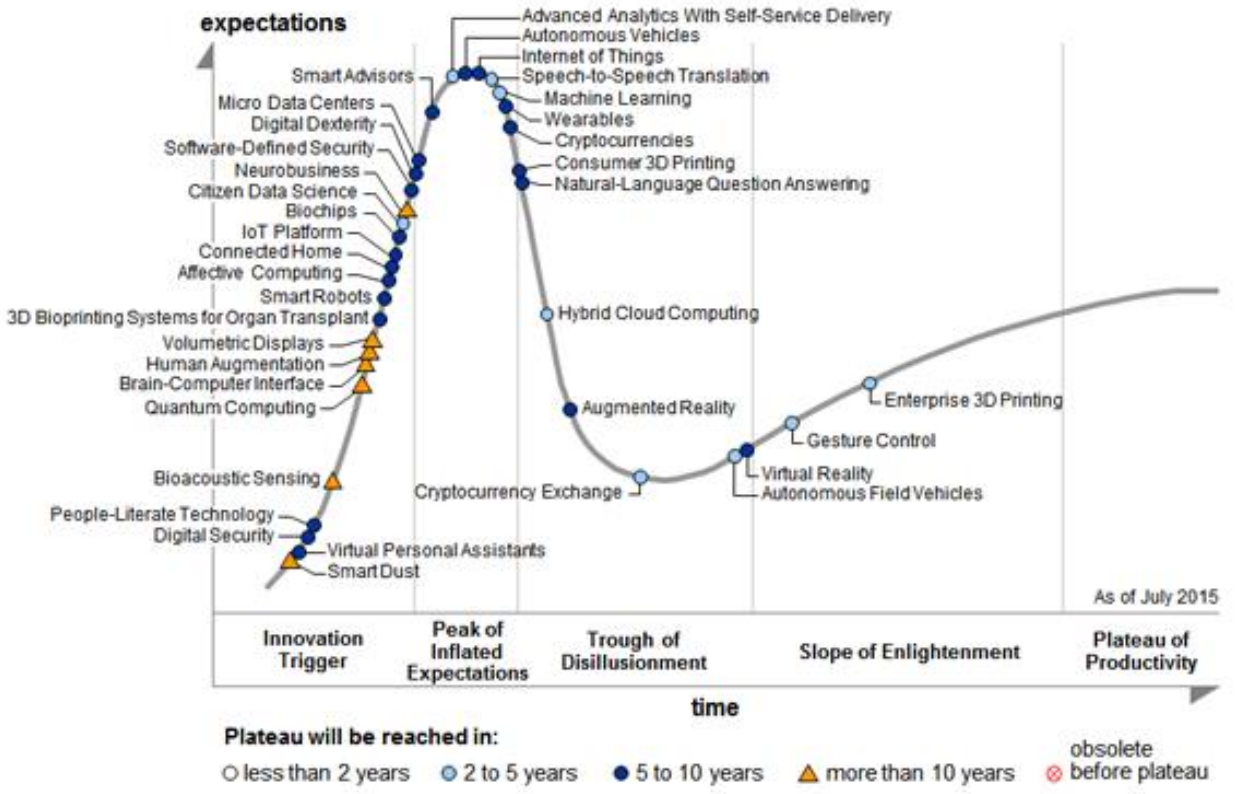

Figure 1 Gartners Hype Cycle 2015

While interest in IoT devices is high, the market for many of its sub-types is embryonic, and adoption rates in the consumer sector seem to be leading the enterprise. In keeping with the perspective that we are currently experiencing the peak of inflated expectations, many crowdfunded IoT projects garnering media attention are undoubtedly more gimmick than pioneering development. Although enterprise adoption may be lagging, the IoT forms a vital part of the blueprint for developing from the digital business model today to the digitisation of the value chain. Spanning manufacturing, logistics, IT, engineering, operations, analytics and sales, the IoT will impact the entire supply chain, alter business strategy and change the job market.

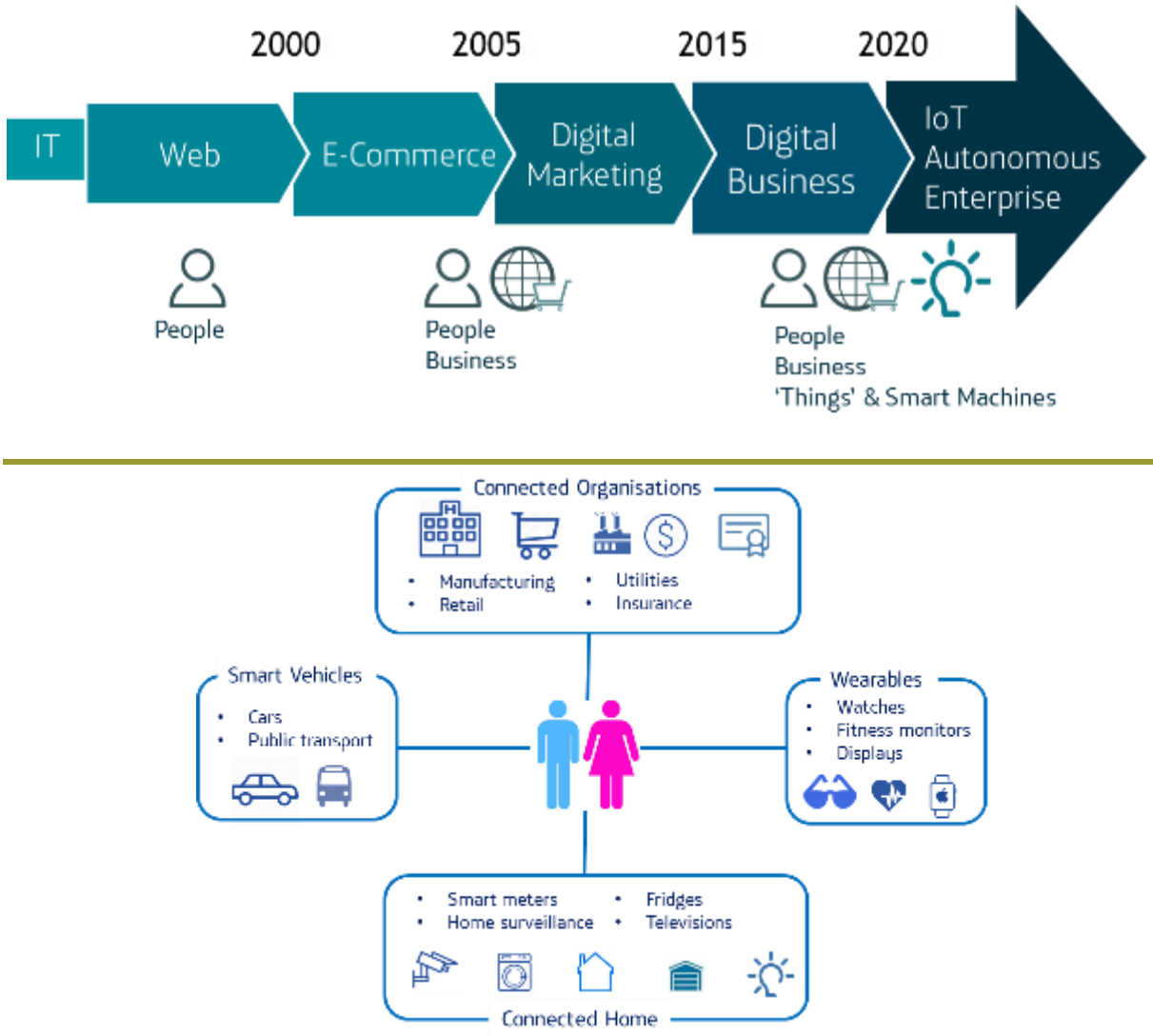

Figure 2. The development of enterprise IoT and wider IoT universe

Within this currently highly fragmented marketplace a number of providers and early adopters across the consumer and enterprise markets are capitalising and seeing measurable benefits from IoT projects. Companies such as Ocado [3], the largest online food retailer in the world have benefited from a business model that has embraced the adoption of IoT before the technologies fully mature. The combination of improved fleet management through tracking vehicle routes, traffic and fuel consumption in real time, alongside automated grocery distribution warehouses, has predominantly been founded on technology that is designed in house. Many other use cases also see companies retrofitting the technology into products that have never before been connected, and not always in an opportunistic sales promotion. Telefónica connected car studies over the past two years have found that the connected car will achieve mass-market penetration in the next few years, and the number of vehicles with built-in connectivity will rise from 10% to 90% by 2020 [4]. For the energy sector smart metering initiatives are a step on the path to developing smart grids, and have seen utility companies planning and implementing projects across the world.

Figure 3. Distribution center run by online grocery retailer Ocado harnessing IoT and AI technology

The Internet of Things Dissected

It is a common media line that the IoT lacks its first 'killer app', but the IoT will not in fact be driven by just one company, it will have to rely on organisations across sectors. Specific expertise and advancements in edge computing, M2M, and the big data fields will have to ensure interoperability to realise the potential of the hype. The IoT cannot be thought of as just a 'Thing' in itself; it is a collection of technologies integrated and presented to provide specific and vastly diverse applications. This is also reflected in how 'smart' the device actually will be, from the 'Dumb' or non-connected, through basic 'smart' monitoring to semi-autonomous, where the device will take some automated action as a response of input to the fully realised fully autonomous IoT device, collecting and processing data, taking action while communicating with other devices autonomously. As devices pass through this IoT maturity lifecycle the risk exposure and potential impact of a security incident increases with capability. The constituent parts of the IoT ecosystem are illustrated in Figure 4.

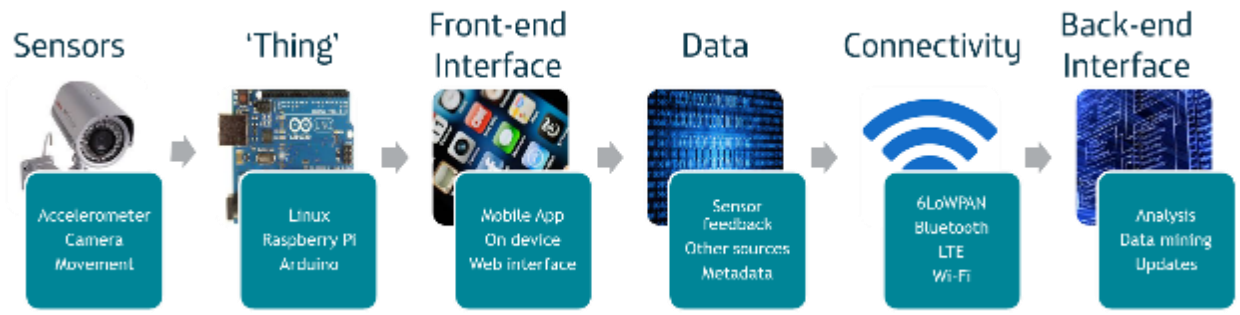

Figure 4. Dissection of an IoT ecosystem

Sensor

Given the disparate user cases for IoT devices the sensor component could be an accelerometer, a camera, a thermometer, or anything providing input to the system. The development and information gathering improvements of sensors must also be considered. As essentially an input field to the network, input should be validated no matter what the devices purpose.

Physical Device aka the 'Thing'

Devices may have wide ranging form-factors, can be anything from embedded Linux, Raspberry Pi, to an AVR microcontroller for example; capable of running software and possessing a network interface, it may just conduct one task or be capable of scheduled tasks. It is important to note that while the device may be purposed for one role it is essentially a standard computing platform technically capable of operating outside the designed parameters. Edge computing advances will distribute processing activity and may be able to significantly reduce the data transmitted as capability improves. The 'Thing' may be intended to be permanently fixed, such as within the connected home, in which case it will reside on the LAN, or in the case of a wearable connect through a mobile device or Wi-Fi.

A generation in many IoT products is likely to be as little as two or three years, but in some cases the dumb 'Things' that are now being made 'smart' with connectivity have very long-lifespans; thermostats or gas meters in the home for example may be unchanged for decades. This naturally opens up problems of technological obsolescence and updates that are a lesser concern to consumer products with a much shorter lifespan. Battery technology will also be a key factor in development, the Apple watch for example requires daily charging, and the trade-off in reducing power usage may see a lot of devices transmitting to a less secure cloud where more resource heavy processing can take place.

Front-end Interface

The manner in which the end-user interacts with the device functionality or service could be done remotely via web or mobile app, such as the Nest Thermostat controls, or alternatively may be embedded within the device itself, as with a smart fridge. Management provides its own challenge, and the market for enhanced home hubs providing a single interface with which to control the various IoT devices around the home is beginning to emerge.

Data

Naturally the diverse use cases across the spectrum of IoT devices means the nature of the structured or unstructured data will be equally varied. However not only will there be great diversity amongst the data types, within the consumer IoT sector particularly there is lot of value that can be derived from the metadata; as opposed to the Industrial Control System (ICS) sector that may just require the feedback from the sensor for example. Devices may also draw information from multiple sources such as databases rather than just an embedded sensor. The inherent storage limitations due to the size of many IoT devices, means this range of data will be stored in private or public cloud services. At this stage of the IoT lifecycle much emphasis is still placed on the physical device, however as the concept matures, increasingly the revenue opportunity would appear to be for related services and monitorization of this data.

Connectivity

The number of devices within a developing IoT ecosystem will quickly run out of IPv4 address space to sate it, so therefore necessitates the uptake of IPv6. Although around for some time, it is not as widely understood as IPv4 and as there begins to be an uptick in the number of devices at some point most infrastructures will need to run IPv6 in conjunction with IPv4. New protocols and standards such as constrained application protocol (CoAP), IPv6 over Low power Wireless Personal Area Networking (6LoWPAN), and 802.11ah 900 MHz WI-Fi will also need to be implemented. It is likely that a number of wireless networking technologies will get traction, and large vendors currently look unlikely to embrace open standards. Designing the architecture for the edge devices, applications, protocols, and analytics capability within this 'system of systems' will certainly be complex. Naturally, within a realised IoT ecosystem the volume of traffic traversing the network will grow exponentially, and already Cisco estimate that global IP traffic will increase 300% to 1.6 zettabytes annually by 2018 [4]. However these wireless technologies are still developing; the 802.11ah standard will not have a certification program for products until at least 2018, so at least for now the focus can remain on existing networks.

Such connectivity implies the need for the 'identity of things', meaning the assignment of unique identifiers with associated metadata to devices, although this uniqueness may only be within a certain context and/or timeframe. This also highlights complexity of the manner in which identity and access management is required to be employed within the IoT. A reimagining of the personal area network is taking place, often with a mobile device doing the local processing and harnessing cloud storage, but established technologies such as Bluetooth are remaining relevant. Finalists in the 2015 Bluetooth breakthrough awards included a connected insulin regulator [5], which although capable of improving quality of life highlights the variety and potential criticality of data that could be contained within an IoT personal area network.

Back-end Interface

The back-end interface enables a control function for service providers to produce, analyse and mine the data. Representing a significant investment for companies to develop in-house, there are IoT management and analytic platforms that can be used as the foundation for application development. Recognising that the maturity of the IoT and the growth of cloud are inextricably linked, leading cloud providers already have prepared their environments with the key features to enable future IoT development.

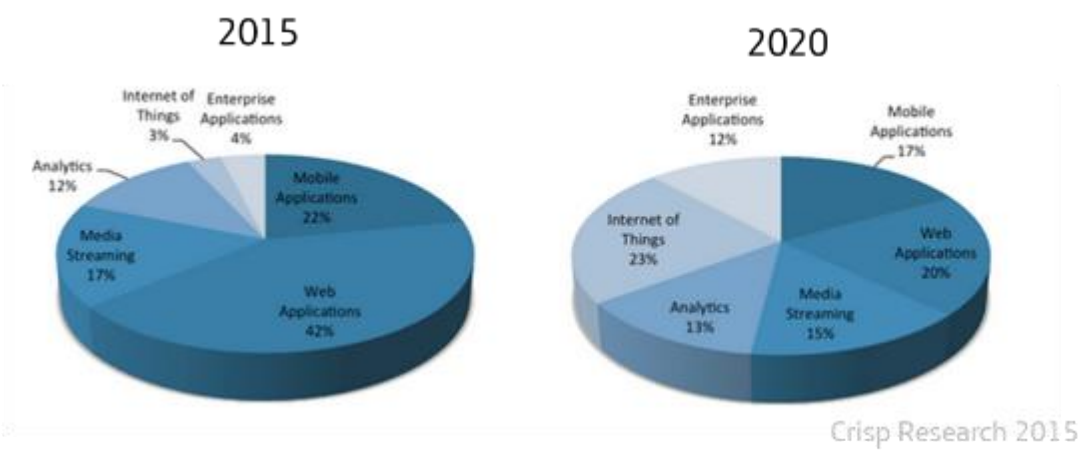

Figure 5. Public cloud usage 2015 and estimated breakdown for 2020

Typical IoT vulnerabilities

It is likely that the IoT will be a highly disruptive combination of technologies, and as with such technological advancement before it, such as cloud computing, the methods adversaries use to take advantage of weakness will be driven by the way the technology itself is implemented. Although the market is in its infancy and will develop over the next 10 years, this emerging field is demonstrating signs of inherent vulnerability currently affecting early adopters.

The human firewall

Before addressing vulnerabilities in technology, it is important to consider human behavioural traits and habits as they may relate to IoT devices. It has become intuitive for employees to be at a heightened state of alert with regard to cyber threats against desktop computers, laptops, and netbooks, but security vigilance often tapers away with regard to mobile devices, or when using corporate IT on public Wi-Fi for example. With IoT devices whose appearance belie the fact it is ultimately still a computer, awareness may increasing fall. The more this IoT ecosystem permeates daily life, the more relaxed people will become with their use, and as a consequence information may be shared over the network that in any other scenario would be more tightly controlled.

Device factors

Small form factors and limited processing and battery power can often inhibit security measures such as the stronger encryption available to larger devices, but as a consequence encryption is often excluded altogether. Research undertaken by HP [7] found that 100% of studied IoT devices in the home security field contained significant vulnerabilities including password, authentication and encryption issues; and this is in a high risk area, during wider testing it was found the average device contained around 20 vulnerabilities. As the ubiquitous and often exposed nature of the IoT also means that the hardware of the devices will be accessible, reducing a key barrier to research, either for legitimate or nefarious means.

Figure 6. Retrofitting IoT connectivity to devices in the home

While no company sets out to make intentionally bad products, manufacturers of general 'dumb' devices with possibly no previous security experience are now making a huge leap to retrofit connected technology into these devices; with many low-cost, or intended to only handle low value data, implementing security is judged as unnecessary expenditure. When highlighted by researchers it is commonly brushed off as an isolated attack by a specialised team, rather than an indicator of a more endemic problem in IoT development [6]. More worryingly, large technology manufacturers are making the same mistakes, in many cases the drive to prove concept before anything else, or attempting to minimise the time to market by doing away with prolonged security testing, seemingly security through obscurity is deemed to be sufficient.

Front-end App implementation

Particularly in the consumer IoT marketplace, devices are controlled through a mobile app with a downloadable APK. It is possible for users to convert and decompile many of these APK's and to view the application source code. Research has shown this is commonly not obfuscated and can contain credentials and encryption keys, as shown in Figure 6, and HP research discovered that 80% of the IoT devices tested along with the mobile and cloud interfaces failed to require sufficient password authentication [8]. Search engines such as Shodan allow anyone to scan for internet connected IoT devices and combined with a lack of basic security methods such as prohibiting brute-force password guessing has caused incidents allowing people to view internal CCTV cameras in a variety of locations [10]. Over the past several years mobile apps have frequently been accused of requesting more permissions than is necessary, and in the IoT marketplace, this trend is often no different, which increases potential risk exposure.

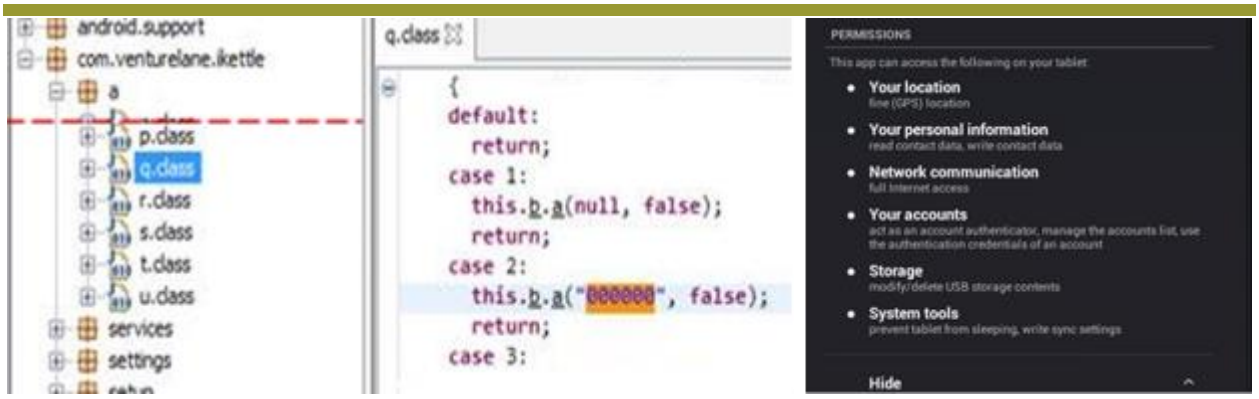

Figure 7. iKettle APK highlighting the default password and an example of requested mobile app permissions

Data storage and the back-end interface

As proposed in Gartner's hype report, the period of inflated expectations of the IoT concept we now witness has lead much of the attention to be focused at the edge device itself. However aside from the headline grabbing edge cases, it is the likely cloud hosted back-end of the IoT ecosystem that will continue to provide the best return on investment for the majority of adversaries. The interconnections within this ecosystem, which will be commonly via API infrastructure are likely to be increasingly targeted. IoT devices often carry inherent difficulties with regard to firmware updates and patching. After media coverage of connected car hacking made headlines in August, Chrysler Jeep posted out USB keys in order to allow users to conduct updates, something that carries inherent risk in itself, and is unlikely to become industry best practice.

Security Implications

The potential benefits of a widespread IoT eco-system are clear, and as the concept must overcome various practical challenges to realise such as vision, it is unhelpful to predict in detail what a world might look like. Future security implications are therefore equally difficult. However given the design and implementation of many IoT devices in the marketplace today have seemingly forgotten the network, application, and cloud security lessons of the past 20 years, general implications of neglecting to ensure security is a key driver in shaping the IoT can be drawn out. While they will depend on the business model, limitations and maturity of the technologies at the time, consequences may manifest themselves across a spectrum of financial, infrastructure, reputational and marketplace risks, summarised in Figure 7, which demonstrate that the IoT risk is far more than an IT issue.

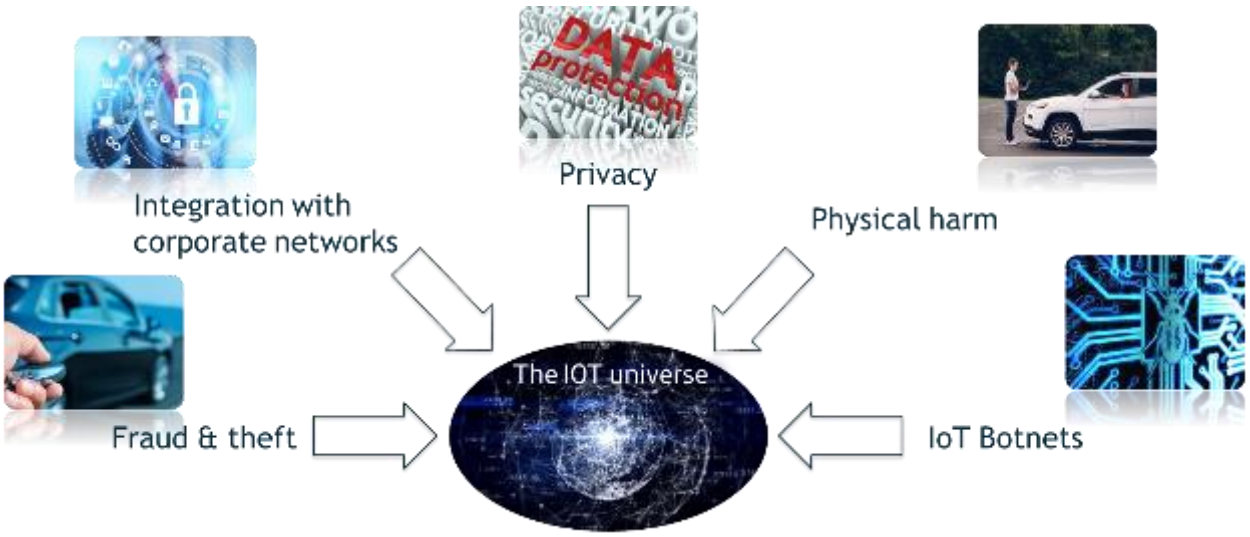

Figure 8. Key areas of IoT risk

Privacy and data protection regulation

Many of the aspirational use cases for IoT devices necessitate collection, storage and transmission of data that is of a personal nature, carrying inherent risk if not handled correctly. The already growing problem of

data aggregation becomes even more pertinent as this data is collected and stored. Questions have already been raised about sensors capturing data about which the consumer is unaware [9], and improving audio visual standards will only add to the collection capability. End-user trust therefore plays an important role, in acting as a bond with the service provider, and subsequently enabling adoption rates to rise. Digital consumer trust surveys [10] have shown this level of trust varies greatly dependant on the age of the end user, and also to a lesser extent on geography (Figure 8). The developing IoT ecosystem will certainly have to tread carefully with consumer trust. Protecting privacy will have to be considered with regard to each component of a system appropriate to its complexity and potential for data manipulation.

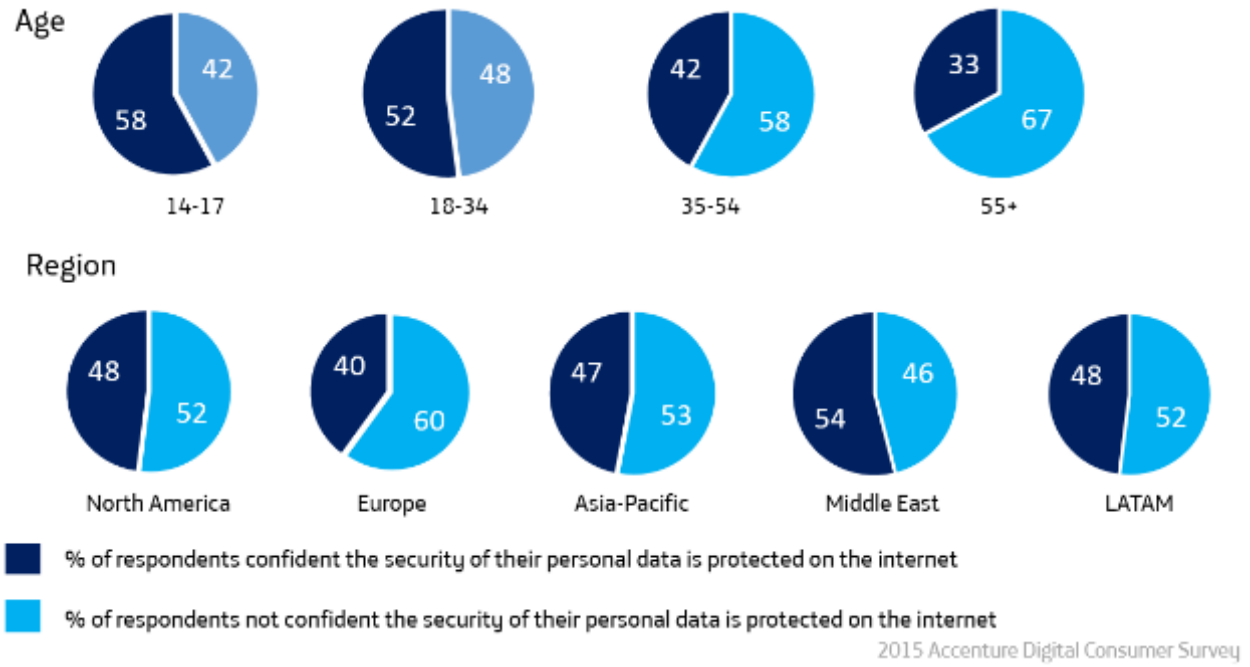

Figure 9. Attitudes regarding personal data on the Internet

Given the speed of innovation and parallels with other fields of technology it is likely that regulatory policy will not be able to keep pace; and a precautionary approach and pre-emptive legislation will be overshadowed by permission-less innovation. Even if this is the case, industry regulators will begin catching up, and without forethought could see an organisation in contravention. Wearables capturing information that could be classed personal medical data, and transmitting to the cloud may be required to be treated in accordance with the appropriate national regulation, such as the Health Insurance Portability and Accountability Act (HIPPA) in the United States, or the relevant EU state law. This has already been recognised in the utilities sector, where guidance from the European Commission [11] regarding the development of smart grids states that European data protection directives are "fully applicable to smart metering systems and smart grids when personal data are processed" [14] . As with many other use cases the European Commission recognises that raising awareness of the technologies assists in fulfilling potential, but in order to gain the necessary level of public acceptance, risks of detrimental usage must also be addressed and mitigated.

Operation within corporate networks

It would be easy for an organisation to assume that information security risk arising from IoT does not apply to them, particularly at the current stage in its lifecycle; however both company and employee owned IoT devices are likely already within the network. Just as BYOD and the widespread use of 'shadow IT' has continued the traditional decline in the IT departments' control and visibility of the network, IoT devices look set to perpetuate this trend. Existing devices may also be potentially more insidious than is realised in many instances. Samsung Smart TV's, in common use in many offices made headlines in February 2015 when the following wording was found in Samsung's' privacy policy; *"Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition."*. Open DNS research [12] discovered that these smart TV's externally communicated to various services almost every minute they are powered on, noting the particular risk that an identifiable pattern of traffic made external identification of the device much easier to determine. As the televisions do not have enough processing power to conduct voice analysis, this feature is conducted remotely and the data was sent in unencrypted form, to and from the device. Employees may introduce personal devices to the network in the form of wearables, but also in a number of other devices capable of processing data. As illustrated in Figure 9 these can have publically available dashboards, in this case displaying environmental data within an office. Equally the confluence of home and office due to changes in working practices are enabling more people being able to do at least some work from home networks that an employer has no visibility of [13].

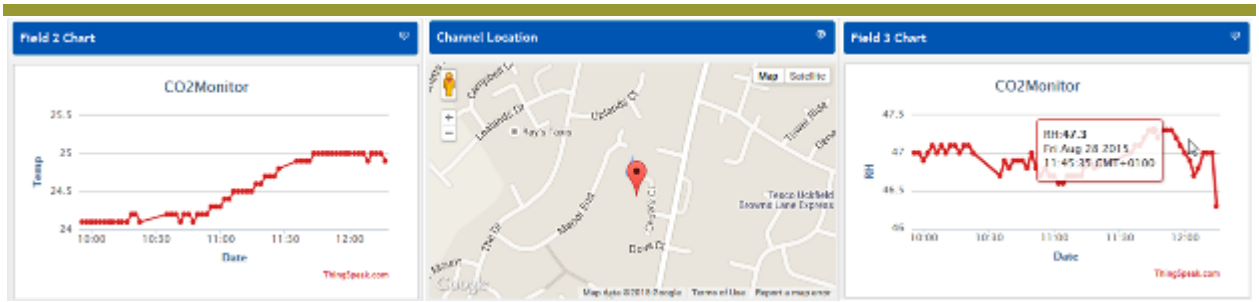

Figure 10. Example publically available IoT dashboard

Risk of physical harm

As the level of scrutiny placed on security dimensions of a device should increase the more capability possesses or sensitive data handled; obviously this too applies to devices that could cause physical harm through failure or manipulation. Currently this risk is most apparent in industrial control systems or medical devices, and is certainly not the priority risk for the vast majority, despite the media hyperbole in the year to date. A security researchers' tweet on hacking avionics mid-flight [14], and remotely taking control of cars through the infotainment system while on public highways (Figure 10) currently represent the edge cases. However as hacking a car illustrates, incorporating seemingly innocuous technological features such as parking cameras and sensors, Bluetooth pairing, or automatically raising the stereo volume at higher speeds, mean control systems may be linked to internet facing entertainment features, and with this comes a level of risk.

Figure 11. Security researchers demonstrate effects of vehicle hacking during the Blackhat and DEFCON conferences

Internet of Things Botnets

The proliferation of IoT devices with public IP addresses and potentially vulnerable operating systems offers a greater attack surface for criminals to manipulate the bandwidth. Just as botnets now are purposed for different goals; Bitcoin mining, cyber-attacks, or installing additional malware, adding more devices to the network will merely offer a greater surface area to target. A report on DDoS attacks during H2 2014 [15] linked an uptick in simple service discovery protocol (SSDP) reflection DDoS attacks to such an increase in IoT devices. More than 30% of compromised devices used to launch attacks were network-connected devices like webcams and home routers, which can be used to amplify the attack by as much as 75 times.

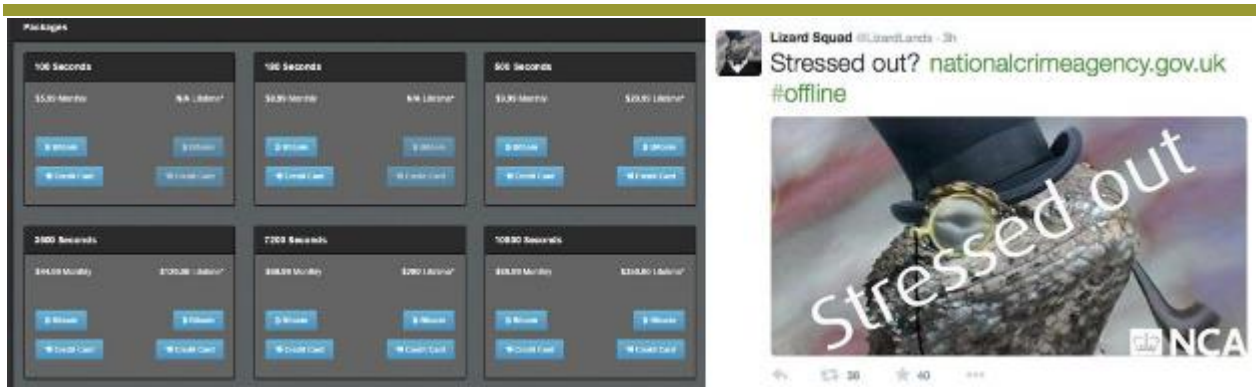

Figure 12. Lizard Stresser website and claims of its use by Lizard Squad

Globally there are estimated to be more than 7 million SSDP devices which could be used to launch such attacks; and this technique has already been adopted by hacktivist groups, and Lizard Squads 'Lizard Stresser' tool is an early example of an IoT botnet used for DDoS attacks. A larger network of hacked IoT devices serving as proxies can also be used by attackers to tunnel attacks through, while benefiting of rapidly changing IP addresses, and research indicates attackers are crawling the internet looking for devices for exactly these purposes [19]. As IoT devices become obsolete and unsupported this will offer even more opportunity, and remediating such attacks if they became more widespread would also be difficult as short term solutions would also likely affect large residential sections of the internet.

Fraud and theft

Additional to monetary loss through loss of service, tampering or fraudulent use of IoT devices is also a key risk for businesses and consumers alike. Utilities companies for instance will have no direct control over a smart meter, and security researchers have already demonstrated the weaknesses in both connected garage doors and connected vehicles. Unanticipated information leakage from the extended IoT ecosystem may also compound the problem of data aggregation which is used by cyber criminals to unite disparate data sets and build comprehensive profiles of potential victims. The utility of this profiling may well develop from the facilitation of further online fraud or access into corporate systems to triggering physical activity such as monitoring IoT home automation systems for certain patterns of behaviour or that might indicate a vacant property.

Increasingly it is likely that the insurance industry will take advantage of the increased data to inform policy premiums, within the connected car market this has already seen a rise in popularity since 2010, illustrated in Figure 12, and in the U.S some employers are holding insured staff to account by giving them fitness wearables [16]. This type of behavioural based insurance has been predicted to become a mainstream form of insurance across Europe [17]. Such developments will undoubtedly be the target of fraudsters, and given the physical connection to the user could equally could be used to track individuals' movement without permission.

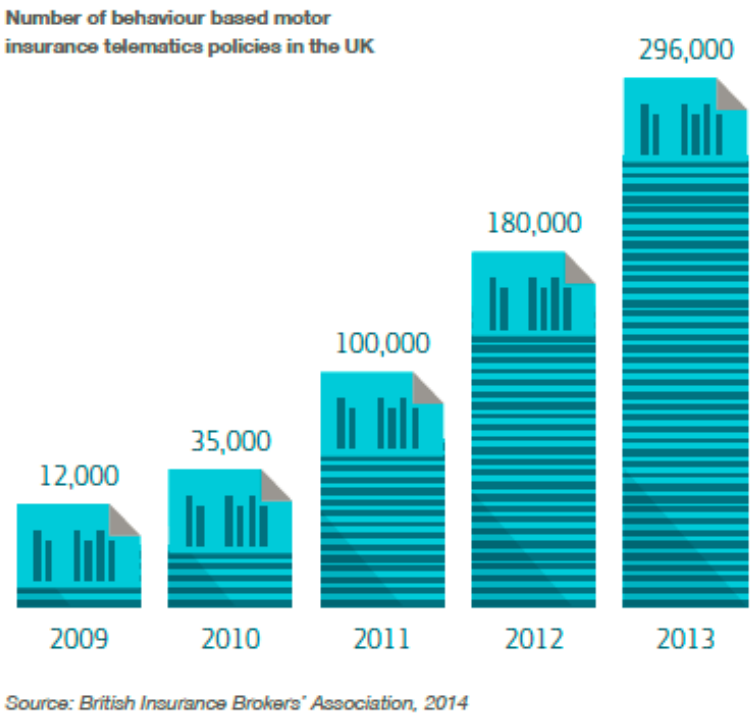

Figure 13. The rise in automotive behaviour based insurance in the UK

Mitigation and countermeasures

While the IoT presents opportunities that can enhance both the consumer and enterprise markets, when striving for the benefits it is prudent for individuals and businesses alike to appraise themsleves of their actual risk exposure when creating or adopting these technologies. Managing initial adoption with insuffucient dilligence could see costs spiraling later as a myriad of security and network issues have to be

dealt with; modelling by RAND suggests that the introduction of IoT could increase the losses that companies experience due to cyber-attacks by 30% over the course of 10 years [18]. As general adoption increases it can also be benefical to take this into account even if there is no policy of IoT implementation, for example, recent media reports highlighted the case of a security firm scanning the 900 MHz band used by IoT devices and discovering that the clients building heating, ventilation and air conditioning (HVAC) system was in fact IoT connected [19] while the client had been completely unaware.

When adopting IoT it is crucial for businesses to factor in security aspects from the start of the initiative. Creation and employment of procurement standards for IoT devices is essential, particularly in this nascent stage of the lifecycle, applying lessons in network, application and cloud security. Risk assessments are naturally contextual to each organisation, the risks in establishing a Smart grid obviously differ from a Smart kettle. As a result, media scrutiny on fields such as connected vehicles have already caused manufacturer recalls; and as a consequence, companies are developing secure telematics and intrusion prevent systems [20] [21] to detect malicious behaviours within vehicle infrastructure. However it important to assess where the most vulnerable components are within the eco-system and this may mean stopping the fixation on the end IoT device. Existing internet facing infrastructure such as cloud databases still contain the sensitive data and may well be the point most at risk, so understanding what an adversary may want to achieve remains important.

Consumer Advice

- Change default passwords on home routers and IoT devices, using the strongest encryption possible when setting up networks, also ensuring device security from the LAN side
- Use devices on separate home network when feasible
- Use strong passwords for device accounts
- Disable or protect remote access to IoT devices when not needed
- Research the vendor's device security measures
- Modify the privacy and security settings of the device to your needs
- Disable features that are not being used
- Install updates when they become available

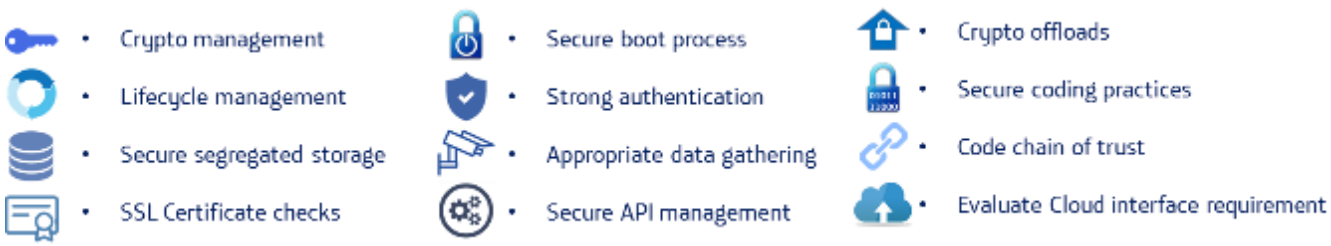

Figure 14. IoT security measures and considerations

As the number and variety of devices becoming connected grows ever more pervasive in daily life it is obvious that not every user will be as technology savvy to instinctively secure devices. Therefore the concept of security by design must be given a higher priority in the manufacturing process in order to avoid security flaws being compounded as the IoT matures. Organisations such as NIST and CNPIC are developing

Cybersecurity Frameworks focused on Critical Infrastructure and Internet of Things, and the OWASP IoT Top 10 provides manufacturers, developers, and consumer's guidance to better understand the security issues when making decisions regarding IoT. Grassroots organisations such as 'Build it secure.ly' and 'I am the cavalry' also exist to promote awareness and best practice with regard to the IoT. Decisions on implementing security measures should also be thought of with the context of the device in mind, as anything too cumbersome will just be circumvented by users.

Manufacturer Advice

- Use secure connections for communication, there are efficient cryptographic methods designed for small scale devices, such as Elliptic Curve Cryptography (ECC)
- Anonymise data where possible
- Allow and encourage the use of strong passwords moving away from 4 number PIN's
- Require the user to change default passwords, do not use hard-coded passwords
- Obfuscate code if users could access it
- Fine-grained consent and access-control rules should be built in
- Provide a simple and secure update process with a chain of trust
- Only gather data that is strictly necessary
- Do not force users to utilise a cloud interface if the device functionality does not warrant it
- Prevent brute-force attacks at the login stage through account lockout measures
- Evaluate device use and consider guidance such as the OWASP Application Security Verification Levels to set requirements and increase aware of the OWASP List of Top Ten IoT vulnerabilities
- Evaluate the quality of Internet IP 'neighbourhood' before setting up platform
- Mutually check the SSL certificate and the certificate revocation list
- Implement a smart fail-safe mechanism when connection or power is lost or jammed
- No open inbound ports
- Code should be verified through a chain of trust
- Use secure boot chain to verify all software that is executed on the device
- Do not transfer data to third parties for additional purposes without explicit approval and segregate data appropriately unless aggregating for analysis purposes

References

[1] Cisco. [Online].

[2] G. 2. H. C. f. E. T. Report. [Online].

[3] Ocado. [Online]. Available: http://www.ocadotechnology.com/our-story.

[4] Cisco. [Online].

[5] Bluetooth. [Online]. Available: http://blog.bluetooth.com/bluetooth-technology-helping-type-1-diabetics-control-insulin-levels/.

[6] B. News. [Online]. Available: http://www.bbc.co.uk/news/technology-31059893.

[7] H. F. o. Demand. [Online]. Available: http://h30499.www3.hp.com/t5/Fortify-Application-Security/IoT-is-the-Frankenbeast-of-Information-Security/ba-p/6705017.

[8] H. I. o. T. r. s. 2014. [Online]. Available: http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

[9] T. P. I. 2015. [Online]. Available: https://www.truste.com/resources/privacy-research/uk-internet-of-things-index-2015/.

[10] Accenture, "Digital Consumer Trust Survey 2015," [Online].

[11] E. Union. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.300.01.0063.01.ENG.

[12] O. DNS, 2015. [Online]. Available: http://info.opendns.com/rs/033-OMP-861/images/OpenDNS-2015-IoT-Report.pdf .

[13] N. Times. [Online]. Available: http://www.nytimes.com/2014/03/08/your-money/when-working-in-your-pajamas-is-more-productive.html.

[14] Wired, 2015. [Online]. Available: http://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/.

[15] NSFocus. [Online]. Available: http://www.nsfocus.com/SecurityReport/2H%202014%20NSFOCUS%20DDoS%20THREAT%20REPORT.pdf.

[16] Forbes, "wearable-tech-health-insurance," 2014. [Online]. Available: http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/.

[17] Telefonica, "M2M Connected Car Report 2014," [Online]. Available: https://m2m.telefonica.com/multimedia-resources/connected-car-industry-report-2014-english.

[18] Juniper Networks & the RAND Corporation, "The economics of defence: Modeling Security Investments Against Risk in an Era of Escalating Cyber Threats," [Online]. Available: http://www.juniper.net/assets/us/en/local/pdf/executive-briefs/3000091-en.pdf .

[19] ITProPortal. [Online]. Available: http://www.itproportal.com/2015/08/02/dangers-of-iot-how-to-mitigate-risks/.

[20] TowerSec. [Online]. Available: http://tower-sec.com/.

[21] Argus. [Online]. Available: http://argus-sec.com/.