Journal of Cyber Policy

ISSN: 2373-8871 (Print) 2373-8898 (Online) Journal homepage: http://tandfonline.com/loi/rcyb20

Security and privacy in the internet of things

Carsten Maple

To cite this article: Carsten Maple (2017) Security and privacy in the internet of things, Journal of Cyber Policy, 2:2, 155-184, DOI: 10.1080/23738871.2017.1366536

To link to this article: http://dx.doi.org/10.1080/23738871.2017.1366536

JOURNAL OF CYBER POLICY, 2017
VOL. 2, NO. 2, 155–184
https://doi.org/10.1080/23738871.2017.1366536

Routledge
Taylor & Francis Group

Security and privacy in the internet of things

Carsten Maple

Cyber Security Centre, WMG, University of Warwick, Coventry, UK

ABSTRACT

The internet of things (IoT) is a technology that has the capacity to revolutionise the way that we live, in sectors ranging from transport to health, from entertainment to our interactions with government. This fantastic opportunity also presents a number of significant challenges. The growth in the number of devices and the speed of that growth presents challenges to our security and freedoms as we battle to develop policies, standards, and governance that shape this development without stifling innovation. This paper discusses the evolution of the IoT, its various definitions, and some of its key application areas. Security and privacy considerations and challenges that lie ahead are discussed both generally and in the context of these applications.

ARTICLE HISTORY
Received 20 April 2017
Revised 5 July 2017
Accepted 8 July 2017

KEYWORDS
Internet of things; security; privacy; trust

Introduction

The internet of things (IoT) is heralded as a development that can deliver dramatic changes in the way we live. It is recognised as an enabler that will increase efficiency in a number of areas, including transport and logistics, health, and manufacturing. The IoT will assist in the optimisation of processes through advanced data analytics, and be the catalyst for new market segments by capitalising on its cyber-physical characteristics, giving rise to cross-cutting applications and services (Miorandi et al. 2012).

The evolution of the IoT

The idea of connecting 'things' to the internet extends much further back than the use of the term 'Internet of Things'. In the early 1980s students at Carnegie Melon University fitted internet-connected photosensors to a soft drinks vending machine, which allowed them to count the number of cans that were being dispensed. This enabled anyone with access to the internet to determine how many drinks had been dispensed, and thus how many were remaining (Vetter 1995).

Even before the first webpage was created, John Romkey and Simon Hackett introduced a toaster that was connected to the internet in 1990. Romkey's presentation at the 1990 Interop Conference featured an internet-connected Sunbeam Deluxe Automatic Radiant Control toaster, and arose as the result of a challenge at the previous year's

CONTACT Carsten Maple cm@warwick.ac.uk

conference from Dan Lynch, President of Interop, to Romkey. Lynch had promised Romkey centre stage at the event if he succeeded. The toaster was connected using TCP/IP and had a Simple Networking Management Protocol Management Information Base (SNMP MIB) controller; its one function was to turn the power on or off. The first use of the term 'Internet of Things' came much later, and is widely attributed to Ashton (Ashton 2009), when he used it as the title of a presentation at Procter and Gamble in 1999.

The growth of the IoT

There has been rapid growth in the number of devices connected to the internet. A number of analysts, notably Cisco and Ericcson (Dave Evans and Hans Vestburg, respectively), have predicted that there will be 50 billion devices connected to the internet by 2020. Of course, these estimates are difficult to assert with confidence, and both have now revised their estimates down. Evans, now at Stringify, predicts 30 million whist Ericcson estimates 28 billion by 2021. One reason that it is difficult to predict growth is that there are not even consistent figures for the number of devices connected to the internet today. Not only is there a significant difference in figures using the same definitions, but the issue concerning the varying interpretations of the IoT also has an impact. Some figures clearly state the difference between machine-to-machine (M2M) and IoT devices, such as those of the GSMA, whose analysis of M2M 'focuses on cellular M2M connectivity and excludes computing devices in consumer electronics such as smartphones, e- readers, tablets, as well as other types of M2M connection technologies that support the wider universe of the Internet of Things (IoT)' (Kechiche 2015). A 2015 report by Machine Research predicted that the total number of M2M connections will grow from 5 billion in 2014 to 27 billion in 2024 (Machina 2015). Nordrum (2016) observed that, in 2016, Gartner estimated that there were 6.4 billion devices (excluding smartphones, tablets, and computers), the International Data Corporation estimated 9 billion (with the same exclusions) and IHS estimated 17.6 billion (including smartphones, tablets, and computers). A similar study by Juniper Research estimated that there were 16 billion devices.

Whilst there are not consistent figures for the number of connected IoT devices, it can be seen that the number of devices is enormous, and growth has been, and is predicted to be, rapid.

Defining the IoT

When writing about his first use of the term IoT, Ashton remarked that the term 'is still often misunderstood'. Indeed, today there exist many definitions and interpretations of the IoT (Atzori, Iera, and Morabito 2010; Bandyopadhyay and Sen 2011; Malina et al. 2016). This might be expected when considering the general public, or researchers with a vague interest in the field, but is more surprising when more specialist researchers vary the definition. For example, the IEEE in its Special Report: The IoT (IEEE 2014) describes the IoT as 'a network of items – each embedded with sensors – which are connected to the Internet'. On the other hand another august, expert organisation, the Internet Engineering Task Force (IETF), states that 'in the vision of the IoT, "things" are very various such as computers, sensors, people, actuators, refrigerators, TVs, vehicles, mobile phones, clothes, food, medicines, books, etc.' (Minerva, Biru, and Rotondi 2015). Following a workshop in 2008,

the Information Society and Media Directorate-General of the European Commission (DG INFSO) and the European Technology Platform on Smart Systems Integration stated that a 'thing' is 'an object not precisely identifiable' (INFSO 2008). Having considered a range of projects involving the IoT, the Strategic Research Agenda of the Cluster of European Research Projects (CERP) on the IoT (Vermesan et al. 2011) gave its own definition of the IoT. This has also been perceived as having shortcomings (Uckelmann, Harrison, and Michahelles 2011) since the definition used components that had been mentioned previously in relation to other visions, such as pervasive or ubiquitous computing, and that this made it difficult to distinguish from these concepts. The IoT can be seen as related to, and emanating from, a number of different technologies, visions, and research directions. Stankovic (2014) has recognised that there is an increasing overlap between, and merging of, principles and research questions in five different research communities: IoT, mobile computing, pervasive computing, wireless sensor networks, and cyber-physical systems. Atzori, Iera, and Morabito (2010) considers the IoT to be the convergence of three key visions: 'things'-oriented (e.g. RFID, NFC, Wireless Sensor Actuators), 'Internet'-oriented (e.g. IP for smart objects) and 'semantic'-oriented (e.g. reasoning over data).

However one considers its evolution, it is clear that the IoT brings together a variety of key areas, and complicating the issue of defining and distinguishing the IoT. Given the close relationship with other visions and advances, and that there is not a common understanding of the definition and size of the IoT, or indeed what 'things' are, it is unsurprising that there are challenges in security, privacy, and policy within the IoT. For the purposes of this paper we will use the interpretation of 'things' as proposed by the IETF.

Relationship to M2M and the internet of everything

Whilst M2M communication is currently a commonly used term, especially given discussion surrounding the Fourth Industrial Revolution and the Industrial IoT, it has a longer history than that. Basic fleet management solutions and Supervisory Control and Data Acquisition (SCADA) solutions have relied on M2M communications for a number of decades (Morrish 2014), and even before this the use of M2M communications allowed the use of ATMs and point of sale systems.

M2M involves direct communication between devices without human intervention. This communication can be over any channel, whether wired or wireless, and the number of technologies, standards, and protocols for communication is large and growing. Communication may occur through a network, including cellular networks (GSM, 3G, 4G), or directly between devices (without going through a base station, intermediary, or access point) in a point-to-point manner, each having a different attack surface. Some of the key communication technologies include Wi-Fi, RFID, Dedicated Short Range Communication (DSRC), Bluetooth, Bluetooth Low Energy (more recently referred to as Bluetooth Smart), NFC, and Zigbee. These technologies vary in frequency, range, and coverage, and are defined by different standards, as presented in Table 1.

In addition to these varying communication technologies, there exist application-specific standards, such as the Meter-Bus standard, developed for the remote reading of gas or electricity meters (EN 13757-x). Within the smart home environment, ISO/IEC have developed ISO/IEC 14543-3 (Home Electronic Systems), and CENELEC (the European

Table 1. Communication technologies used in IoT and M2M systems.

Technology	Standard	Frequency	Coverage	Bit rate	Comments
WiFi	IEEE 802.11	2.4/5 GHz	50 m	500 Mbps	High consumption
ZigBee	IEEE 802.15.4	2.4 GHz	100 m	250 kbps	High security
Z-Wave	ZAD12837	900 MHz ISM	50 m	40 kbps	Home automation
Sigfox	Sigfox	900 MHz ISM	10 km	1 kbps	Low consumption
Neul	Neul	458 MHz	10 km	100 kbps	Low-cost IoT
LoRaWAN	LoRaWAN	ISM bands	15 km	50 kbps	Wireless battery operated IoT
RFID	ISO/IEC 18000	LF, ISM bands	<2 m	40 kbps	
NFC	ISO/IEC 18092	13.56 MHz	<20 cm	424 kbps	
GSM/3G/4G	GSM, UMTS/HSPA, LTE	900/1800/1900/2100 MHz	50 km	10 Mbps	High consumption
Bluetooth LE	IEEE 802.1	2.4 GHz	50 m	1 Mbps	Low consumption
6LoWPAN	RFC6282	ISM bands	n/a	n/a	
HomePlug	IEEE1901	<100 MHz	<100 m	10–500 Mbps	Smart grids
Thread	Based on IEEE802.15.4	2.4 GHz	<100 m	250 kbps	Up to 250 devices
DSRC	IEEE802.11p	5 GHz ISM	300 m	27 Mbps	V2V comms
WiMax	IEEE802.16	2.3, 2.5, and 3.5 GHz	10 km	10 Mbps	

Committee for Electrotechnical Standardization) have developed EN 50090-x (Home and Building Electronic Systems).

It should be noted that there exist a variety of internet of X descriptions: ABI research (ABI 2017) thinks of the IoT as a parallel development to the Internet of Humans and Internet of Digital, for example. Buxmann et al. discuss the development of the Internet of Services (Buxmann, Hess, and Ruggaber 2011), whilst ABB has been developing products and services for the IoT, Services and People. The Fourth Industrial Revolution is being developed through the Industrial IoT (Sadeghi, Wachsmann, and Waidner 2015), the connected car agenda is developing into the Internet of Vehicles (Gerla et al. 2014), and there are even more obscure developments such as the Internet of Animal Health Things (Smith et al. 2015).

Recently, Cisco and Qualcomm have been advocating the use of the term internet of everything (IoE). Whilst some argue that this term may have been developed as a marketing ploy by Cisco, there is certainly some benefit in defining a system that goes beyond many of the typical uses of the IoT, especially given its development outside of M2M environments. As M2M can be considered a subset of the IoT, the IoE can be thought of as a superset of the IoT.

The concept of the IoE brings together four key elements: people, process, things, and data. Here the *things* are physical sensors, devices, actuators, and other items, generating data or receiving information from other sources. Rather than being restricted to the human, we can consider the human-generated and -related systems such as social networks, and health, well-being, and fitness applications. Data are analysed and processed to create useful information for intelligent decisions and to control mechanisms. This concept of the IoE will not only allow examination of the IoT as a system involving machines and humans, but also brings together the services, context, environments, and intelligence – the data and the process (Bojanova, Hurlburt, and Voas 2014). In the context of the IETF definition of the IoT, this vision of the IoE might be considerably less of a fundamental shift.

To summarise, the IoT has evolved using a wide range of core technologies from a number of key visions. It has evolved through developments by distinct, often disparate communities, each with slightly different overarching aims. Further, these developments

have been made in different application areas, often using specific and proprietary standards. This diffuse nature of development has led to an inevitable lack of harmonisation and shared vision, hampering standardisation and effective regulation. It is this lack of standardisation and regulation that has precipitated many of the existing security and privacy issues in the IoT, and left technicians and users without the necessary information and control to, service, update, and address problems created with devices and services. The lack of coherence, oversight, understanding, and protocols means that security risk analysis, risk assessment, and countermeasure implementation are much more difficult tasks than they would be with a more directed and coordinated development path. The nature of the growth, both rapid and significant, has meant that the impact of these concerns is considerable and requires urgent redress.

In this paper we present a discussion of the security and privacy challenges in the IoT, illustrated through a number of key applications. The paper first presents an overview of the widespread applications of the IoT and the various classifications of applications found in the literature. It outlines a number of specific application areas, before presenting a discussion on general security and privacy issues in the IoT. The impact of the IoT on security and privacy concerns are then discussed, before the final conclusions and recommendations in areas of key concern are made.

Applications of the IoT

The IoT is having a significant impact in a number of domains, and a number of researchers have provided insights and analyses into its applications. When presenting applications of the IoT, researchers have their own classification of domains and applications. Each taxonomy has its own merits, and depends not only upon the objective to be achieved but also the definition and context of the IoT under consideration. The reader is referred to the references presented in Table 2 (further information on the applications of the IoT).

Application domains have been presented by both industry and academia. For example, the industry brochure, Libelium (2015), lists 61 applications for the IoT in a number of domains using different sensor boards. Academic efforts include Atzori, Iera, and Morabito (2010) who classify applications in four short-medium term categories (transportation and logistics; healthcare; smart environment – home, office, plant; personal and social) and a longer term futuristic category. In Miorandi et al. (2012) the authors use six categories, retaining the healthcare domain whilst modifying others. Most significantly, however, they overlook the personal and social domain, and instead introduce the security and surveillance category. Whitmore, Agarwal, and Xu 2015 use a modified classification based upon consideration of an updated literature review, drawing most significantly on the work of Atzori, Iera, and Morabito (2010) and Miorandi et al. (2012). This classification dispenses with a temporal futuristic view and reorganises the transportation and logistics and smart environment domains, recognising the considerable role of the IoT in supply chains and its connection to the field of logistics, thus developing a category specifically for supply chains and logistics. Further, a new category, smart infrastructure, is presented, which extends the smart environments domain of Atzori and introduces the infrastructure aspects of transport. Zanella et al. (2014) focus attention on the smart city whilst Da Xu, He, and Li (2014) concentrate on industry applications of the IoT, and include consideration of the niche case of the IoT as applied to firefighting. Authors of

Table 2. IoT domains and key applications mentioned in the literature.

Paper	Domains	Key applications
Atzori, Iera, and Morabito (2010)	Transportation and logistics	Logistics; assisted driving; mobile ticketing; environment monitoring; augmented maps
	Healthcare	Tracking; identification and authentication; data collection; sensing
	Smart environment (home, office, plant)	Comfortable homes and offices; Industrial plants; Smart museum and gym
	Personal and social	Social networking; historical queries; losses; thefts
	Futuristic	Robot Taxi; City Information Model; Enhanced Game Room
Perera et al. (2014)[b]	Industry	Supply chain management; transportation and logistics; aerospace; aviation; automotive
	Society	Telecommunication; medical technology; healthcare; smart building; home and office; media; entertainment; ticketing
	Environment	Agriculture and breeding; recycling; disaster alerting; environmental monitoring
Whitmore, Agarwal, and Xu (2015)	Smart infrastructure	Smart grids; smart homes and building; smart air quality; Intelligent traffic system; smart parking; waste management
	Healthcare	Monitoring health; assisted living; medical practices
	Supply chain and logistics	Tracking products (RFID sensors); reducing counterfeiting; product traceability
	Social application	Integration with Facebook, Twitter; location-based interest; contact synchronisation.
Da Xu, He, and Li (2014)[a]		Healthcare service; food supply chain; safer mining; transportation and logistics; firefighting
Farooq et al. (2015)		Smart traffic system; smart environment; smart home; smart hospitals; smart agriculture; smart retailing and supply chain management.
Li, Da Xu, and Zhao (2015)	Industrial; social IoT; healthcare; infrastructure; security and surveillance	
Bandyopadhyay and Sen (2011)[b]		Aerospace and aviation; automotive; Telecommunications; medical and healthcare; independent living; pharmaceutical; retail, logistics and supply chain management; manufacturing; Process; environment monitoring; transportation; agriculture and breeding; media, entertainment industry; insurance; recycling
Vermesan et al. (2011)[b]		Aerospace and aviation (systems status monitoring, green operations); automotive (systems status monitoring, V2V and V2I communication); telecommunications; intelligent buildings (automatic energy metering/home automation/ wireless monitoring); medical technology, healthcare, (personal area networks, monitoring of parameters, positioning, real-time location systems); independent living (wellness, mobility, monitoring of an ageing population); pharmaceutical; retail, logistics, supply chain management; manufacturing, product lifecycle management; processing industries – oil and gas; safety, security and privacy; environment monitoring; people and goods transportation; food traceability; agriculture and breeding; media, entertainment and ticketing; insurance; recycling

(*Continued*)

Table 2. Continued.

Paper	Domains	Key applications
Al-Fuqaha et al. (2015)		Smart home; smart building; intelligent transportation system; industrial automation; smart healthcare; smart grids
Zanella et al. (2014)	Smart city	Structural health of buildings; waste management; improved air quality; noise monitoring; traffic congestion; city energy consumption; smart lighting; automation and salubrity of public buildings
Libelium (2015)	Smart cities	Smart parking; structural health; noise urban maps; smartphones detection; electromagnetic field levels; traffic congestion; smart lighting; waste management; smart roads
	Smart environment	Forest fire detection; air pollution; snow level monitoring; landslide and avalanche prevention; earthquake early detection;
	Smart water	Portable water monitoring; chemical leakage detection in rivers; swimming pool remote measurement; pollution levels in the sea; water leakages; river floods
	Smart metering	Smart grid; tank level; photovoltaic installations; water flow; silos stock calculations
	Security and emergencies	Perimeter access control; liquid presence; radiations levels; explosives and hazardous gases
	Retail	Supply chain control; NFC payment; intelligent shopping applications; smart product management
	Logistics	Quality of shipment conditions; item locations; storage incompatibility detections; fleet tracking
	Industrial control	M2M Applications; indoor air quality; temperature monitoring; ozone presence; indoor locations; vehicle auto-diagnosis
	Smart agriculture	Wine quality enhancing; green houses; golf courses; meteorological station network; compost; hydroponics
	Smart animal farming	Offspring care; animal tracking; toxic gas levels
	Domestic and home automation	Energy and water use; remote control appliances; intrusion detections systems; art and goods preservation
	eHealth	Fail detections; medical fridges; sportsmen care; patients; surveillance; ultraviolet radiations
Miorandi et al. (2012)	Smart homes/smart buildings; smart cities; environment monitoring; healthcare; smart business/inventory and product management; security and surveillance	

[a]Paper focuses on IoT in Industries.
[b]Perera et al. and Bandyopadhyay and Sen draw heavily on the CERP-IoT, hence similarities between the three.

this latter paper extend their work to wider applications (Li, Da Xu, and Zhao 2015), combining it with concepts from Atzori and Miorandi. Perera et al. (2014) and Bandyopadhyay and Sen (2011) both draw heavily on the report from the CERP into the IoT (Vermesan et al. 2011). This report defines three essential application domains for the IoT: industry, environment, and society. However, the report finds that it is difficult to isolate any of these domains, and rather applications and services apply at the intra- and inter-domain level. Instead, we should consider applications (which support one or more of the aforementioned domains) and services that cater for a specific functionality or need

at an intra- or inter-domain level. Therefore, if organisations wish to consider their cyber security risk, to do so at the domain level would be misleading, though apparently intuitive. The fact that there exist a number of ways to consider domains and applications should tell us that this way of thinking about risk is unhelpful. Whilst threat modelling and risk assessment across domains can have similar *themes*, they are likely to have radically different *risks*. Thus, rather than considering cyber security risk at domain level, we should examine a number of IoT applications that are at the inter-domain level. We now discuss a small selection of applications that carry significant cyber security risk, representing high impact and/or likelihood of an attack.

Connected and autonomous vehicles

The application of sensors in the automotive sector has been one of the largest growth areas (Meola 2016). There are a significant number of sensors within vehicles used for everything from engine operation to system monitoring, emission control, and brakes. Examples include Bluetooth-enabled tyre pressure monitoring systems, crank position, cam position, manifold absolute pressure, and throttle position. Sensors are also being embedded to form an integral part of transport infrastructure, and there has been significant investment in the UK with, for example, the introduction of Highways England's Smart Motorways Programme (Phull 2012). Other initiatives include developing infrastructure and communication in urban environments. UKCITE (www.ukcite.co.uk) is a project in the UK funded through both the Centre for Connected and Autonomous Vehicles and Innovate UK (part of a £100 million investment programme in research and development) that involves equipping over 40 miles of urban roads, dual-carriageways, and motorways with communications technology. Using Vehicle to Infrastructure (V2I) communication allows better traffic flow, especially in urban and suburban environments (Faezipour et al. 2012). Communication between vehicles, so-called V2V communication, through technologies such as DSRC, long-term evolution for vehicles, and Visible Light Communications, are enabling the platooning of cars in order to reduce energy consumption and provide advance notice of incidents. The deployment of such Intelligent Transportation Systems utilising Edge and Cloud Technology can assist in accident management, location-based traffic, and weather notifications, thereby supporting assisted driving (Atzori, Iera, and Morabito 2010).

Health, well-being, and recreation

The use of sensors is an integral part of emerging medical and healthcare technologies. The IoT has the potential to be integrated into numerous healthcare services and applications (Dohr et al. 2010; Bui and Zorzi 2011; Islam et al. 2015). The healthcare services that will benefit most significantly include ambient assisted living (a significant area of application involving the use of smart homes to allow patient monitoring and care in independent environments); the internet of mobile health (integrating medical sensors into mobile technologies); semantic medical access (utilising semantics, IoT healthcare applications can use medical rule engines to analyse large quantities of sensor data); and adverse drug reaction (by labelling drugs and examining a medical database, any potential adverse reaction such as allergy, or reaction with other drugs, can be

avoided). Healthcare applications that have already been developed, or are set to be developed include blood pressure and diabetes monitoring, body temperature and rehabilitation monitoring, oxygen saturation monitoring, and wheelchair management (Stachel et al. 2013).

Industry 4.0

One of the biggest impacts globally of the IoT is expected to come through the advent of the Fourth Industrial Revolution, in which IoT technologies are to be incorporated into each phase of the manufacturing process. This will involve a shift from automated to intelligent manufacturing processes (Thoben, Wiesner, and Wuest 2017), incorporating cyber-physical systems, automated robotics, big data analytics, and cloud computing (Fedorov et al. 2015). The IoT can be employed throughout the development lifecycle through the introduction of smart connected machines with proactive maintenance, enabling a smarter manufacturing process delivered through intelligent logistics, allowing rapid, flexible, and lean manufacturing. Optimised decision-making and innovative planning methods, combined with smart grid technology, will mean the energy efficiency of plants can be maximised.

Logistics

With large numbers of shipments and increased inventory, IoT technologies can support logistics dynamically by enabling the service provider to increase operational efficiency whilst also increasing automation and decreasing manual processes (Macaulay, Buckalew, and Chung 2015). The uses of the IoT in logistics can have a pronounced impact on smart inventory management, damage detection, real-time visibility, accurate inventory control, optimal asset utilisation, predictive maintenance, and freight management (Uckelmann, Harrison, and Michahelles 2011). The application of RFID technology to logistics (Sun 2012) enables industry to forecast information, identify future trends, estimate the probability of an accident, and allow for the early adoption of remedial measures. This can improve enterprises' ability to respond to the market and maintain risk aware supply.

Smart grid

In recent years there has been a dramatic increase in investment in smart grid research and development, pushing the UK into the lead in the European deployment of a wide range of viable smart grid solutions (DECC 2014). Smart Grid is an intelligent power system which incorporates information and communication with existing transmission and distribution systems (Li et al. 2011). This is made possible by utilising sensors, digital meters, and controllers with analysis tools to monitor and optimise grid performance, prevent power outages, and restore supply (Li et al. 2011). The development of Smart Grid will help cater to the requirements of smart cities with numerous intelligent systems creating building and community energy management systems (CEMS) (Karnouskos 2010). The IoT sensors can help identify devices connected to the grid and send real-time power information to the consumer.

Homes, buildings, and offices

There has been a significant growth in the demand for smart home devices, with over 161 million units being shipped between 2010 and 2016 according to IHS Markit (IHS 2016); over half of these devices were delivered in 2016, a 64-per cent increase on the previous year. This increase included purchases of smart energy management systems such as Nest thermostats, security solutions such as August smart locks, and personal home assistants such as Google Home, Bosch's Mykie, and Amazon's Alexa.

In addition to growth in consumer adoption of smart technology, there has also been a surge in demand within the office environment. A new report by British Land and Worktech Academy (British Land 2017) of over 1000 workers, nearly a third of whom were decision-makers, found that 88 per cent of respondents expressed a wish to control their work environment better. The study found that a smart office would have a significant impact on company performance and environment, with predictions of productivity increases of 37 per cent, loyalty increases of 38 per cent, and well-being and happiness improving by over 40 per cent. This growth in demand for the IoT in houses, buildings, and offices will contribute to the development of smart cities (Zanella et al. 2014).

Retail

With the increased benefits of sensor technologies, the IoT has the ability to enhance the consumer experience in retail stores and businesses. Monitoring and controlling operational data and equipment performance, for example, will allow businesses to improve performance by tracking progress in real time (Lee and Lee 2015). Sensors generate large quantities of data through time, which can be used to determine potential drawbacks and help businesses adapt through big data and business analytics. Understanding the market trends and demands of customers through advanced market analysis will lead to reactive and proactive supply, which can limit resource wastage and developments that will ultimately fail to find demand. Through increased adoption of the IoT, not only can retailers ensure appropriate procurement and supply, but also offer customers different products, which may be more suited to their needs. For example, a user may buy some consumer electronics, but there may be products that can offer the appropriate amount of interoperability, battery life etc. as an alternative. This decision could be derived from information gathered from sensors, and could work in much the same way as when we choose to update our mobile telephone or internet packages, receiving advice from suppliers regarding the most appropriate service for our needs. Customer satisfaction can also be achieved through connected retail, as well as customer recognition and context aware offers (Macaulay, Buckalew, and Chung 2015).

Agriculture

Smart technology is also being developed in the agricultural sector. Field information is traditionally obtained through manual reporting mechanisms, which can lead to inaccuracies in data. To maximise and streamline the production of agricultural commodities by systematically increasing efficiency and decreasing manual labour, IoT sensors and technologies can contribute to scientific cultivation with increased quality (Chen and Jin 2012). This is

enabled through monitoring environmental parameters such as air pressure, humidity, and wind direction through wireless sensors, which can help cultivation through the adaptation of agricultural requirements. Furthermore, from production processes through to market consumption, the food supply chain requires the maintenance of appropriate preservation techniques which can be improved through sensor technologies and pervasive computing (Atzori, Iera, and Morabito 2010). The importance of food traceability was highlighted in the Elliot Review (Elliott 2014). The IoT can play a significant role in improving assurance, logistics, and supply chain management through tracking and tracing systems.

Entertainment and media

Entertainment and media is also seen as a sector which could benefit from the advances in the IoT (Martin 2016), and research is being developed for media content sharing services over home-based IoT networks (Hu et al. 2013). This provides an ability to both personalise content seamlessly and allow the simple sharing of media. Advertisements can be personalised for individual communities and families. Potential content filtering based on age is also expected to have an impact on the entertainment industry (eMarketer 2016). Other applications, such as ad hoc news gathering based on the location of the user, are also set to increase (Bandyopadhyay and Sen 2011). The games industry is a significant area of the entertainment sector, and one in which the IoT could have a considerable impact. We have already seen the huge popularity of Pokémon Go, and the combination of the IoT and augmented reality systems could play a major part in the development of new gaming experiences.

Security challenges within the IoT

As the IoT expands and becomes more interwoven into the fabric of our everyday lives, as well as becoming an increasingly important component of our critical national infrastructure, securing its systems becomes vital. The securing of systems can be based upon a number of principles, from the CIA of information security (confidentiality, integrity, and availability), to the five pillars of information assurance (confidentiality, integrity, availability, authenticity, and non- repudiation) and the Parkerian Hexad (confidentiality, integrity, availability, authenticity, possession, and utility) (Parker 1998). Research articles discussing security considerations relating to cyber-physical (as opposed to information) and IoT systems vary in which principles they adopt. The majority of researchers restrict consideration to the CIA. The Parkerian Hexad, whilst originally offered as an improvement to overcome the limitations of the CIA, is often rejected; indeed, the usefulness of the Hexad remains the subject of debate among security professionals (Feruza and Kim 2007). Others go beyond these earlier principles and include robustness, reliability, safety, resilience, performability, and survivability (see for example Sterbenz et al. 2010). It is certainly worth considering all of these components of security, especially in complex cyber-physical systems such as the IoT. However, for this piece we use the three broadest categories of the CIA, understanding that the compromises may be of physical as well as information assets. We discuss some of the most significant challenges, highlighting which principles are under threat of compromise. However, it must be recognised that this is not an exhaustive list of the security challenges.

Physical limitations of devices and communications

In any application area, IoT devices are usually embedded with low power and low area processors, and it has been recognised that 'the Internet Protocol could and should be applied even to the smallest devices' (Mulligan 2007). Constraints on IoT devices limit the ability to process information at speed – there is a limited CPU, memory, and energy budget. This means that challenging forms of security are required which satisfy the competing goals of strong performance and minimal resource consumption. The constraints in size and power impact most significantly on efforts to maintain confidentiality and integrity in IoT systems. For example, the largest physical layer packet in IEEE 802.15.4 (recall that Zigbee and 6LoWPAN, for example, are both based on this standard) is 127 bytes (Montenegro et al. 2007). Given that the frame overhead could be 25 bytes, the maximum frame size in the media access control layer is 102 bytes. To protect confidentiality encryption can be applied, but it should be noted that link-layer security further reduces this maximum frame size. If AES-CCM-128 (Advanced Encryption Standard using 128 bits, running in so-called CCM mode, a mode of operation designed to provide both authentication and confidentiality) were to be used, this would consume 21 bytes, leaving only 81 bytes available. On the other hand, using AES-CCM-32 would only consume 9 bytes, leaving 93 available. Designing appropriately secure and robust systems is challenging, since communication between nodes is often over 'lossy and low-bandwidth channels' (Heer et al. 2011).

For security through digital signatures, a public key infrastructure is required, and this is a significant challenge to IoT systems. Public key infrastructure can protect against both loss of confidentiality and loss of integrity. However, even the encryption process with the public key requires computational and memory resources that are beyond many wireless sensor systems, especially when frequent data transmission is required (Doukas et al. 2012).

Heterogeneity, scale, and ad-hoc nature

It has been recognised that the high level of heterogeneity (Sicari et al. 2015; Misra, Maheswaran, and Hashmi 2016), compounded by the large scale of IoT systems, will magnify security threats to the current internet. Roman, Najera, and Lopez (2011) notes that heterogeneity has 'great influence over the protocol and network security services that must be implemented in the IoT'. Security solutions have to cope with entities with varying hardware specifications, and need to provide authentication and authorisation of IoT nodes (Malina et al. 2016), as well as key agreement (Suo et al. 2012). The heterogeneity of the IoT means it cannot be assumed that all devices can present a full protocol stack. Further, the potential number of services and service execution options, along with the need to handle heterogeneous resources, requires service management; these challenges will have an adverse impact on the security of IoT systems (Miorandi et al. 2012). The lack of open standards and use of proprietary solutions presents a significant problem, since security solutions must integrate with 'black boxes'. Allowing developers to implement security based on their own proprietary standards can lead to 'security through obscurity' (Phillips, Karygiannis, and Huhn 2005), recognised as a flawed technique within the ambit of security. Security issues are further exacerbated due to the fact that 'transient and

permanent random failures are commonplace, and failures are vulnerabilities that can be exploited by attackers' (Stankovic 2014), and that the ad hoc nature of the IoT requires the tailoring of existing techniques (Sicari et al. 2015). Clearly, as the number of devices connected to the internet grows, so do security and privacy issues (Cha et al. 2009).

Many components of the IoT, particularly in the health and transport and logistics domains are also mobile. This presents a challenge in ensuring that security solutions adapt to the mobile environment, interacting with many different components and systems, each potentially offering different settings, protocols, and standards.

Authentication and identity management

Identity management concerns the unique identification of objects, and authentication then validates the identity relationship between two parties (Mahalle et al. 2010). The CERP report (Vermesan et al. 2011) recognises that further research is needed in the 'development, convergence and interoperability of technologies for identification and authentication that can operate at a global scale'.

Authentication within the IoT is critical, since without appropriate authentication the confidentiality, integrity, and availability of systems can be compromised. This is because if an adversary can authenticate as a legitimate user, they will have access to any data that the user has, and can see (compromising confidentiality), modify (compromising integrity), and delete or restrict availability (compromising availability) in the same way that the user can.

The authentication and identification of *users* in the IoT remains a significant challenge. Currently, username/password pairs are the most common form of authentication and identification of users in electronic systems, though other forms such as shared keys, digital certificates, or biometric credentials may be used (Gessner et al. 2012). However, the vision of the IoT as ubiquitous will eliminate many of the physical interaction interfaces through which usernames and passwords are passed.

In traditional electronic environments the ability to take advantage of single-sign-on (SSO) mechanisms can be useful, allowing users to authenticate only once to interact with various services. Systems such as Shibboleth OpenID and OAuth2 were not designed to fulfil IoT systems, and whilst work is being undertaken to adapt OAuth2 it cannot, as yet, provide widespread SSO in IoT environments. Citizens in an IoT environment may wish to choose their identity provider, and this is challenging using current protocols.

Furthermore mobility, privacy, and anonymity require further analysis and research (Riahi et al. 2013). Those IoT systems that feature mobile services will have users passing through different architectures and infrastructures owned by different providers. Managing the identity of users in such mobile, heterogeneous, and multiply owned environments can be challenging. Whilst privacy in the IoT is discussed in the next section, the issue of anonymity in the IoT presents a particular challenge, especially in mobile environments. Although there may be a desire for anonymity, users also want good levels of service, and this often requires understanding as to 'whom' the service is being provided. Furthermore, if there is a need for resilient services, then accountability is desirable. Clearly, in a truly anonymous system, accountability is hard to achieve. Pseudonymity can provide a balance between anonymity and accountability. In pseudonymous systems, the actions of a person are linked to

a random identifier, rather than an identity. A pseudonym may provide a persistent identifier to ensure that a service can be offered from initiation to completion. To be effective in IoT systems, there remains a challenge for pseudonyms to operate in a standardised manner across multiple domains.

It is not just the identification and authentication of users that requires consideration. It is also necessary to identify and validate service and devices in IoT systems. It can be challenging to perform a *strong* authentication of devices in the IoT 'because of the nature of the device or the context in which it is being used' (Sarma and Girão 2009). Without adequate authentication processes, it is not be possible to assure the data originated from the intended device, or was received by the intended device. If the devices are appropriately authenticated, there is still a requirement to authenticate the service, since certain services will have access to certain data.

Authorisation and access control

It has been recognised that there is a need to 'exercise access control over [the Internet of Things] at the edge of the network in the device or, at least, a local access controller for the device' (Cerf 2015). There is an important role in establishing whether the user, once identified and validated, has permission to access the requested resources (Abomhara and Køien 2014). Access control requires communication between entities (often restricted to software entities rather than human, since users impact on the system through the software entities that they control) to request and grant access. There are various models for access control such as Discretionary Access Control (DAC – where an administrator determines who can access resources); role-based access control (RBAC – allowing access based on the role that the requester holds); and attribute-based access control (ABAC – where rights are granted through policies which evaluate the attributes of the user, resource requested and the environment from which the request is made).

Effective access control in an IoT context is challenging. Whilst it is desirable to use an access control model that removes discretion, the use of RBAC and ABAC is known to be challenging for low-powered IoT devices. Further, RBAC requires the definition of roles. In many IoT systems there is the likelihood that the number of roles will grow rapidly, and thus handling all these roles, especially during system updates, becomes difficult if fine-grained access control is intended. ABAC faces similar challenges, especially in decentralised architectures. Neither ABAC nor RBAC 'provide scalable, manageable, effective, and efficient mechanisms … and [so] are not able to effectively support the dynamicity and scaling needs of IoT contexts' (Gusmeroli, Piccione, and Rotondi 2013). RBAC, ABAC, and DAC are all access control list (ACL) models, and an alternative approach is to use capability-based approaches. These methods involve the requester having a reference or capability that allows access to a service. This requires a reference that is communicable, revocable, unforgeable, and which can be thought of as analogous to the key to a safe deposit box. These methods attempt to overcome some of the limitations of ACL models, but they are unable to 'tailor access based on various attributes or constraints' (Ferraiolo, Cugini, and Kuhn 1995). Capability-based methods include identity authentication and capability-based access control (IACAC) (see Mahalle et al. 2013), and capability-based access control (CapBAC) (see Gusmeroli, Piccione, and Rotondi 2013).

Implementation, updating, responsibility, and accountability

It is vital, though often overlooked in discussion, that the implementation and updating of security protection must be both manageable and low cost. IoT systems can be geographically remote and involve sensors and actuators in extreme and challenging environments. To protect the cyber security of the system it is vital that any vulnerabilities are addressed as soon as they are discovered. As such, there is a need for remote access to allow these system updates. The latest software patches could be installed dynamically, and the process managed through cloud-assisted frameworks; however, designing a secure mechanism for dynamic installation is a challenging task (Maglaras et al. 2016). It must also be recognised that updates can change the functionality of devices, and these changes may not always be aligned with user expectations (Rose, Eldridge, and Chapin 2015). For this reason, in cases where a user has responsibility or control over applying a patch, they may decide against updating if they feel the risk of compromise outweighs the negative impact on functionality (Cavusoglu, Cavusoglu, and Zhang 2008). The Dyn attack in 2016 was illustrative of the significant impact a botnet of the likes of unpatched printers, IP cameras, residential gateways, and baby monitors can have in conducting a distributed denial of service attack. This leads to another significant challenge regarding responsibility, liability, and accountability in the IoT. Since the IoT, comprises different devices, communications, infrastructure, and services under different control and ownership, determining responsibility and liability remain a challenge. Whilst legal liability may lie with one organisation, the impact of a seemingly innocuous attack on one component could cause catastrophic, irrevocable damage to another. For example, if a service is compromised due to an issue in a device or some third-party architecture, the repercussions in terms of customer backlash may not impact on the device manufacturer or architecture owner, but rather the service operator. The possibility of such cases may lead some parties to be less concerned about cyber-physical security than they should be. The situation is even more difficult given the highly complex attack surface. One minor vulnerability in one device or service may be exploited along with other, seemingly innocuous vulnerabilities elsewhere in the system, controlled, owned or supplied by different parties. If this leads to a major compromise, the level or responsibility of each party may not be immediately clear. This makes it difficult to make a case for security investment.

Security issues in connected and autonomous vehicles

The connected and autonomous vehicles (CAV) area is complex and involves many different sensors, actuators, infrastructure, communications protocols, and services. These services vary from small, simple services running on only a few components, through to global services involving significant parts of the critical national infrastructure. This work cannot encompass all of the types of system and potential and implemented attacks. However, it is possible to highlight some of the most significant attacks.

Modern vehicles have between 70 and 100 integrated electronic control units (ECUs) for applications such as braking, steering, transmission, suspension, and engine control. The sensors providing information into these ECUs include the Tyre Pressure Monitoring System Infotainment system, Camera, LIDAR, RADAR, and brake and engine sensors. Communication to ECUs is through a range of network types including CAN (Controller Area

Networks), FlexRay, MOST (Media Oriented System Transport), and LIN (Local Interconnect Network). Different manufacturers employ different networks, but modern vehicles will feature a number of these network types. However, these protocols were designed prioritising efficiency and safety rather than security. Checkoway et al. (2011) and Koscher et al. (2010) exploited various on-board and remote vehicular vulnerabilities physical endpoint devices such as On-Board Diagnostic Units (OBD), and external communications such as DSRC and Bluetooth. More publicised was the work of Miller and Vallesek in 2015, in which they used remote execution to exploit a vulnerability (combined with a weakness in the Sprint-enabled remote access UConnect®) in a Jeep Cherokee (Mansfield-Devine 2016). They were able to control the vehicle whilst it was in motion.

Although the likelihood of a cyber-attack on a connected vehicle is currently thought to be low, the increasing importance of these vehicles, and the rise of technologies such as ransomware, make this a significant emerging risk to the integrity and availability of connected and autonomous vehicular systems. As well as financial motivations, we are likely to see attempts to compromise these systems by terrorists, nation states, and hacktivists.

Many applications in CAV involve a combination of personal and vehicular (that can be linked to individuals) data that is sent externally. This type of data can have its confidentiality and privacy breached in a number of ways, including through the use of 'sniffing stations'. It is also possible to undertake man in the middle attacks on the wireless communications entering a vehicle, thereby compromise the integrity of that data. Such a man in the middle attack was the basis of the remote exploit of the Jeep by Miller and Valasek.

As connected vehicles interact with and become dependent upon infrastructures such as Cloud and Edge-cloud, the risk and impact of attacks on the availability of systems will increase.

Security issues in health, well-being, and recreation

Recently, there have been an increasing number of attacks where the victims have been hospitals. There have been a myriad of potential and actual attacks on individual connected devices, including drug delivery systems, electronic health implants, insulin pumps, and pacemakers. However, recent years have seen attacks being discovered that are unprecedented in their scale and surface. In particular, the MEDJACK attack (Storm 2015), first discovered by Trend Micro, impacted on blood gas analysers, computerised tomogram apparatus, magnetic resonance imaging systems, and x-ray machines. Attacks have been carried out that targeted communications protocols as well as devices. Security flaws have been found in the proprietary communication protocols of ten implantable cardiac defibrillators (ICDs) (Marin et al. 2016). These medical systems obviously pose a risk to each part of the CIA triad. As well as the very evident problems of disrupting availability and compromising integrity, there are also issues of confidentiality. Medical data can be used for identity theft or fraud, as well as to discover drug prescriptions, enabling hackers to order medication online. Hackers might also consider extortion and blackmail of people with certain illnesses that they would not want disclosed. Similar attacks on the confidentiality, integrity, and availability of IoT-enabled well-being, such as fitness trackers, also exist, though the impact from breaches on availability and potentially integrity is less severe. This is not the case regarding confidentiality of information.

Security issues in Industry 4.0

Industry 4.0 has been heralded as a transformational move that brings together data, connectivity, and autonomy to create the Fourth Industrial Revolution. However, there exist a number of significant threats to these cyber-physical systems.

Significant cyber-physical attacks have been reported over a number of years, and there are likely a significant number of attacks that are not reported, or even discovered. Examples include the Maroochy Water Services attack in Australia in 2000, in which the sewerage system encountered a series of faults where the pumps were not running when they were supposed to be and alarms were disabled. This was further aggravated by a loss of communication from the central computer with various pumping stations. Similarly, Stuxnet had a rapid and significant impact on the Iranian nuclear industry. More recent attacks include the 2014 attack on a German steel mill, and disruptions to the Ukrainian energy network.

Other attacks on confidentiality of information include leakage of intellectual data that can lead to the loss of competitive advantage in the market. In addition, it would also equip competitors with the capacity to undermine innovations that are yet to be manufactured.

Security issues in logistics

The IoT appears to offer significant efficiency and business opportunity in logistics. There are various application scenarios, which inevitably creates a large attack surface. One recognised attack is the manipulation of embedded data, either by malicious substitution of tags or by modification of tag information (Misra, Maheswaran, and Hashmi 2016). Whilst logistics are often thought of as part of the road network, it should be recognised that logistics also involve rail, air, and sea. A particular vulnerability concerns the modification of ship details including position, course, cargo, flagged country, speed, name, and MMSI (Mobile Maritime Service Identity) status (Balduzzi, Pasta, and Wilhoit 2014). To further intensify an attack, the creation of fake vessels with all the same details of an existing vessel can be exploited, for example, having an Iranian vessel with nuclear cargo appear off the coast of the US. This compromises the confidentiality and integrity of the system.

Security issues in smart grid

Attacks on critical national infrastructure for energy, such as the reported attack by China and Russia on the United States (see Misra, Maheswaran, and Hashmi 2016), and the attacks on Ukraine have been discussed extensively in white papers, academic papers (see Liang et al. 2017) for example, and the wider press. These attacks are predominantly (though it may be argued not exclusively) attempting to disrupt availability in these cyber-physical systems. However, there are a number of other attacks known within Smart Grid technologies.

Attacks are not always at the national infrastructure level, but can occur further down the architecture. CEMS are more localised, and are used to determine and balance community power requirements, including deciding the size of generators and the capacity

of transmission lines to be used over short periods of time to meet demand. CEMS have already been shown to be vulnerable to denial of service attacks as well as counterfeit messaging, compromising both availability and integrity.

Further down the architecture there is a significant growth in the rollout of smart metres. UK government figures state that by September 2016 there were over 500,000 smart metres installed in the UK. However, data transmitted over the internet by the smart meters have been shown to be unsigned and unencrypted (Greveler et al. 2012), compromising the confidentiality of the system.

Security issues in homes, buildings, and offices

There is a vast range of devices for the smart home promising intelligent resource efficiency through remote and instant access and control. Whilst such devices and services offer economic and functional benefits, they do increase security risks. The key risks that such devices represent are to confidentiality and privacy. Some issues, such as how energy consumption can provide inferences for profiling, have been discussed previously. So, too, have the use of connected home devices and their contribution to the Dyn attack. The types of devices that have been compromised already include cameras, printers, doorbells, weighing scales, and recently, in the UK in particular, home routers, among many others. Whilst lack of availability of these devices is inconvenient, when the power of all devices is combined into a botnet, the global impact can be significant.

As well as attacking the devices in smart homes and offices, hackers will target the building automation and control systems. Probably the most significant attack utilising access to internet-connected building control systems was the attack on Target. The attack originated by compromising the heating, ventilation, and air conditioning (HVAC) company supplying Target. The company will have had access to the Target network for remote monitoring and maintenance, and this will have provided an entry point into the system that the attacker could escalate from, thereby compromising the confidentiality of 40 million customer records. Of course, access to building systems for homes or offices carry a wider threat not just to confidentiality, but also to integrity and availability.

Privacy challenges in the IoT

Privacy is seen as a major concern in the IoT (Misra, Maheswaran, and Hashmi 2016; Sicari et al. 2015; Ziegeldorf, Morchon, and Wehrle 2014; Roman, Najera, and Lopez 2011; Gessner et al. 2012). The IoT has made an enormous quantity of data available, belonging not only to consumers such as is the case with the World Wide Web, but to citizens in general, groups, and organisations. This can be used to establish what we are interested in, where we go, and our intentions. Whilst this can provide great opportunities for improved services, it must be weighed against our desire for privacy. It is vital that consumers trust the services they engage with to respect their privacy. Trust is a fundamental element in the forming of any relationship, and is a vital factor in the adoption of new technology (Yan, Zhang, and Vasilakos 2014). People will not use new technology if they do not have sufficient trust in the safeguarding of privacy, security, and safety (Taddeo and Floridi 2011; IBM Watson Foundation 2015), and this is particularly true in complex systems such as the IoT.

Sensors, including those embedded in mobile devices, collect a variety of data about the lives of citizens. This data will be aggregated, analysed, processed, fused, and mined in order to extract useful information for enabling intelligent and ubiquitous services. Trust refers to the determining of when and to whom information should be released or disclosed (Yan and Holtmanns 2008).

In 2010 Facebook founder Mark Zuckerberg proudly stood on stage and announced that 'privacy is no longer a social norm'. This has been debated at length by a number of academics. In 2006, a privacy paradox was proposed (Barnes 2006), arguing that 'adults are concerned about invasion of privacy, while teens freely give up personal information'. This central thesis has been the subject of a great deal of academic work (it has in excess of 900 citations), with many academics demonstrating that this paradox exists in various contexts. However, changes have been observed, and recently the Oxford Internet Institute released a report that detailed a *new* privacy paradox. In the report, Blank, Bolsover, and Dubois (2014), argue that young people 'are much more likely than older people to have taken action to protect their privacy', and that the new paradox is based upon the notion that 'social life is now conducted online and that SNSs do not provide users with the tools that would adequately enable them to manage their privacy in a way that is appropriate for them'. A recent study by Pew Research Center (Rainie et al. 2013) found that 86 per cent of internet users have taken steps online to remove or hide their digital footprints. Techniques employed included clearing cookies, avoiding using their real name, encrypting email and using virtual networks to hide their internet protocol (IP) address.

Giving users more control over the collection and use of their personal information has been seen as an essential aspect of ensuring trust in distributed systems. Previous projects, such as the Platform for Privacy Preferences Project (P3P) have been designed to give users control when using web browsers. The P3P protocol, an initiative of the World Wide Web Consortium (W3C) initiated in 2002, allows websites to declare the intended use of data collected through web browsers. It was built upon the idea of translating website privacy policies into standardised machine-readable information to aid transparency and enable user choice. Unfortunately, the project ended prematurely, and there have been very few implementations. There are a number of reasons cited for the failure of P3P, centred around the lack of adoption by industry and users (Jøsang, Fritsch, and Mahler 2010). Specific reasons include a lack of adoption by websites (Reay et al. 2007) due to the drivers for businesses to adopt PET technologies (compliance, efficiency, and risk of brand damage) are not significant enough for a sufficient number of businesses (Beatty et al. 2007); a lack of adoption by browsers (Cranor et al. 2008); and a lack of acceptance by users, including cultural considerations that affect the international adoption of P3P (Reay et al. 2007; Reay, Dick, and Miller 2009).

A variety of privacy enhancing technologies have been developed for ensuring privacy, including Virtual Private Networks, Transport Layer Security, DNS Security Extension, Onion Routing, and Private Information Retrieval (Weber 2010). Privacy Policy Languages are another type of PET, and the P3P project discussed earlier can be considered to belong to the PET class of PPLs (Wang and Kobsa 2009). PPLs can be categorised as *external* (declarative without enforcement) or *internal* (normative with support for enforcement); P3P falls in the former class. Other PPLs include SAML (Security Assertion Markup Language), XACML (an OASIS standard for access control), including PPL, A-PPL, and

GeoXACML the extensions of XACML; XACL; SecPAL and its extension for specifying the handling of personally identifiable information, SecPAL4P; AIR (Accountability In RDF); XPref; P2U; EPAL; P-RBAC; FlexDDPL; Jeeves; PSLang; ConSpec; and SLAng (see Kasem-Madani and Meier 2015 and Henze et al. 2016 for more information). Whilst there exists a range of PPLs, none has emerged as the de facto standard, and large-scale adoption remains a challenge.

Consent

As mentioned previously, it is important to balance optimised and personalised service with the desire for privacy. One method of reconciling these competing objectives is to ensure the consent of the consumer to their data to be collected, stored, and shared. However, this brings about a number of challenges. Consent has traditionally been based on a system of transparency: a provider of a service should make clear what data is collected and what it is to be used for. Of course, there have been questions about whether presenting a consumer with 70 pages of detail is clear in itself, and this is now starting to be addressed by regulation. The draft General Data Protection Regulation (GDPR) Consent Guidance Document from the ICO in the UK (ICO 2017) states that whilst the Data Protection Directive stated that 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed', Article 4(11) of the GDPR states 'any freely given, specific, informed and *unambiguous* indication of the data subject's wishes by which he or she, *by a statement or by a clear affirmative action*, signifies agreement to the processing of personal data relating to him or her'. If the IoT realises the vision of becoming ubiquitous, we will be interacting with systems without a physical interface. In this case (as noted by Peppet 2014), 'giving consumers data and privacy information and an opportunity to consent is particularly challenging'. The GDPR (2016) also requires consent to be granular and easy to withdraw. These are significant challenges with the absence of suitable interfaces to provide or revoke consent. These challenges will not only be in public areas, but within homes as IoT technology becomes embedded. For example, the data from the pressure sensors, IR sensors, and RFID systems are sufficient for an adversary to monitor and understand the human activities in a home. As an example, data associated with a smart fridge could be used to determine eating habits and health which, might affect the individual's life insurance with an insurance company. The use of sensors and intelligence is also growing in the production of toys. Smart toys have the ability to recognise the voice of, analyse, and interact with the child. These toys usually have external Bluetooth and Wi-Fi connection capabilities, which leaves the endpoints vulnerable to adversarial attacks (Dobbins 2015). These toys can expose children's personally identifiable information, and also leads to the fear of the children's location being tracked and making them vulnerable. In addition, these toys can be used to act as surveillance devices, or hijacked to behave inappropriately (Chaudron et al. 2017). This leads to the challenge for toymakers to incorporate security from the inception of connected toys (Nelson 2016). Parents who give children smart toys are either implicitly or explicitly giving consent for the data pertaining to their child to be collected, processed, stored, and transmitted. However, they are not, in general, empowered to consent to the handling of data of other children, a friend say, interacting with the toy. Without this explicit consent

the personal data of the friend should not be handled. However, separating the two sets of data will be challenging, and it is likely that toys will handle data without explicit consent.

Privacy concerns within the IoT are not restricted to consumers, there can also be impacts on industry. The Industrial IoT is more complex than traditional ICT systems, due to the large attack surface with numerous attack vectors (Sadeghi, Wachsmann, and Waidner 2015). A proper definition of the privacy requirements needs to be formulated (Da Xu, He, and Li 2014). Beyond the risk of violation of sensitive employee or customer details, the potential loss of intellectual data opens up the possibility of competitors replicating the knowledge and capabilities of the victim organisation, which can undermine competitive advantage (Sadeghi, Wachsmann, and Waidner 2015). Whilst it is understood that industrial espionage, through an inside or other attack, can result in intellectual property theft, there are cases where indirect privacy compromises could lead to a leakage of intellectual capital. For example, if the data related to industrial orders are compromised, it not only gives a competitor the ability to predict the industrial supply of current goods and materials, but also future goods and innovative technologies currently in development. Similarly, data protection compromises could reveal the financial performance along with the business processes and business intelligence of an industry which could restrict the industry's ability to borrow money, or impact on its insurance premiums. This area has received little attention as yet.

Conclusions and further work

In this article we have discussed the origins of the IoT and how this has posed a major challenge to standardisation and a single overall vision. This, in turn, has given rise to challenges for security and assurance in the IoT.

Arguably the most significant challenge, but also the most fundamental, is to encourage standardisation and coordination in the IoT. This is not only difficult in terms of process and technology, but also politics. There needs to be consideration of all stakeholders and their conflicting views on the IoT. The P3P project shows the difficulties involved in gaining consensus and trust between parties that have different visions and interests.

The P3P project was laudable but faced considerable difficulties. An analogous system for the IoT would certainly be beneficial, but it is challenging to ensure that the outcomes are relevant and acceptable to all. If there is to be a protocol, analogous to P3P, to *communicate* how data are captured, processed, stored, and transmitted, and offer users a way to have *choice and control* regarding their data, it is important that lessons are learned from the P3P project. It is important that, for any standard to be successful, the project should be mindful of the politics involved. Privacy advocates may see the development as industrial subterfuge, a criticism that was levelled at the P3P project; the protocol should not allow services to create an illusion of privacy whilst gathering personal data. It should be recognised that any standard is likely to be only part of a solution, and as such, implementing the standard alone may not provide adequate protection. Therefore it is recommended that the standard should be used together with other privacy enhancing tools. Any standard should be developed in line with legal and regulatory compliance. If there is no compliance requirement or financial implication to not implementing the protocol, the business case for the protocol will fail. To maximise the

probability of industry adoption and user acceptance, any protocol for managing consent in the IoT should be:

- developed around firmly agreed principles, to ensure there is no mission creep and that the objectives are clear;
- simple, economically efficient, and implementable;
- mindful of any impact on current and future business models;
- co-developed with industry bodies (service and infrastructure providers) and user representative groups;
- developed in line with legal and regulatory compliance. If there is no compliance requirement or financial implication to not implementing the protocol, the business case for the protocol will fail.

Another key area that requires immediate attention is in the low power and low area (small form factor) aspects of the IoT. Challenges exist in developing attack-resistant solutions on such constrained devices, and an ability to *detect*, *diagnose*, and *recover* from attacks.

Key protocol developments to address the problem of strong, low-budget security include the work of the IETF 6LoWPAN group, who have developed encapsulation and header compression mechanisms that allow IPv6 packets to be sent and received over low-rate wireless personal area networks. Nodes in these IEEE 802.15.4-based networks can operate in two secure modes: *ACL mode* (providing access only to trusted nodes) and *Secure mode* (providing confidentiality, message integrity, access control, and sequential freshness). Other protocols that are designed to address such issues include Host Internet Protocol (HIP), and Datagram Transport Layer Security (DTSL). The former is more efficient but the 'limited usage of HIP poses severe limitations' (Garcia-Morchon et al. 2013), whilst the latter is more interoperable, but offers poor performance. Key management, including storage and exchange, remains a significant challenge for resource-constrained IoT systems, as many current solutions for security rely on firmware with significant energy consumption overheads (Healy, Newe, and Lewis 2009).

Authentication and identification in IoT systems is fundamental for security and privacy. Obviously, systems based upon biometric identification, possibly combined with a token, may prove advantageous compared to existing systems, but care must be taken to ensure that the system is secure yet frictionless.

Significant progress has been made in the battle to ensure the authenticity of devices, streams, and services in the IoT. In particular, the development of Physical Unclonable Functions (PUFs) (see Suh and Devadas 2007; Tuyls and Škorić 2007; Guajardo, Kumar, and Schrijen 2007), can play a role in device authentication. A PUF has a complex and unpredictable yet repeatable mapping system of inputs to outputs. For efficient authentication, the function needs to be easy to evaluate and repeatable, and for security purposes it needs to be difficult to predict. Some weaknesses have been observed, such as ageing, which can make PUF responses unreliable (Maiti and Schaumont 2011), and improved schemes using enhanced challenge-response are being developed (Maiti, Kim, and Schaumont 2012). PUFs are being combined with embedded Subscriber Identity Modules (eSIMs) to provide authentication and access control. The eSIM is used to address issues of scalability, interoperability, and compliance with security protocols (Cherkaoui, Bossuet, and Seitz 2014).

Other areas requiring urgent attention include the need to adapt existing SSO mechanisms, or create new ones that better fit the IoT. Although some approaches address this need, proposing a hybrid architecture that combines all mechanisms through specially crafted middleware [6], this topic still needs research.

There is also a need for a standardised communication platform and architecture, with unified security considerations in intelligent transport systems, prioritising the incorporation of security in each layer of the architecture. Attacks have been shown to be feasible from the physical layer (through communications such as Bluetooth or DSRC), through to the network layer (such as CAN, LIN etc.), to the facilities layer by altering the ECUs, before finally affecting applications such as windscreen wipers and door locks.

Various Industrial IoT attacks have also shown SCADA vulnerabilities such as slow updates and authentication holes, paving the way for further attack vectors on the network. This raises a need for secure and reliable architecture that can protect an Industrial IoT from network to endpoint devices, which governs the functioning of an industry.

The IoT presents an opportunity to revolutionise the way we live and work. However, there remain a number of significant challenges to ensure that its potential can be realised without catastrophic consequences. There are numerous guidelines and best practices for security in the IoT available to individuals and organisations. The U.S Department of Homeland Security (DHS 2016) explains the risks and strategic principles of the IoT, and suggests best practices for devices and systems from design to operational. The Broadband Internet Technical Advisory Group (BITAG 2016), provide a, report that highlights the issues associated with general consumers installing IoT products by analysing and emphasising issues such as data leaks and privacy violations. Specific security requirements for connected vehicles and medical devices are recommended by the group *I Am The Cavalry* (Cavalry, 2014, 2016). In the cellular domain, GSMA has produced a comprehensive overview report that investigates the availability, identity, privacy and security challenges of the IoT, presents guidance on the mobile solution and provides examples in different applications (GSMA Association 2016a). The overview report acts as a primer to the Service Ecosystem (GSMA Association 2016b) and Endpoint Ecosystem Reports (GSMA Association 2016c). The final report in the suite outlines security principles for network security, privacy considerations and the services provided by network operators (GSMA Association 2016d). Even with the guidance available, there remain challenges around the design, implementation, and management of the IoT. In this paper we have discussed some of these challenges, from defining and standardising the IoT, to specific challenges such as eliciting and managing consent. It is clear that significant progress is being made, but there is still a long way to go in the battle to secure the IoT.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by Cyber Security of the Internet of Things [EPSRC Grant EP/N02334X/1].

Notes on contributor

Professor Carsten Maple leads the GCHQ-EPSRC recognised Academic Centre of Excellence in Cyber Security Research at the University of Warwick, where he is Professor of Cyber Systems Engineering and Director of Research in Cyber Security in WMG. Professor Maple has published over 200 peer reviewed papers and is co-author of the UK Security Breach Investigations Report 2010, supported by the Serious Organised Crime Agency and the Police Central e-crime Unit. His research has attracted millions of pounds in funding and has been widely reported through the media. Professor Maple is the Privacy and Trust stream lead for PETRAS, the UK Research Hub for Cyber Security of the Internet of Things. He is currently funded by a range of sponsors including EPSRC, EU, DSTL, the South Korean Research Agency, Innovate UK and private companies.

References

ABI Research. 2017. "What Is the Internet of Things?" Accessed July 4, 2017. https://www.abiresearch.com/pages/what-is-internet-things/.

Abomhara, Mohamed, and Geir M. Køien. 2014. "Security and Privacy in the Internet of Things: Current Status and Open Issues." International Conference on Privacy and Security in Mobile Systems (PRISMS), Aalborg, Denmark, May 11–14, 1–8.

Al-Fuqaha, Ala, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. 2015. "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications." *IEEE Communications Surveys & Tutorials* 17 (4): 2347–2376.

Ashton, Kevin. 2009. "That "Internet of Things" Thing." *RFiD Journal*, 97–114.

Atzori, Luigi, Antonio Iera, and Giacomo Morabito. 2010. "The Internet of Things: A Survey." *Computer Networks* 54 (15): 2787–2805. doi:10.1016/j.comnet.2010.05.010.

Balduzzi, Marco, Alessandro Pasta, and Kyle Wilhoit. 2014. "A Security Evaluation of AIS Automated Identification System." Proceedings of the 30th Annual Computer Security Applications Conference, New Orleans, LA, December 8–12, 436–445.

Bandyopadhyay, Debasis, and Jaydip Sen. 2011. "Internet of Things: Applications and Challenges in Technology and Standardization." *Wireless Personal Communications* 58 (1): 49–69. doi:10.1007/s11277-011-0288-5.

Barnes, Susan B. 2006. "A Privacy Paradox: Social Networking in the United States." *First Monday* 11 (9). doi:10.5210/fm.v11i9.1394.

Beatty, Patricia, Ian Reay, Scott Dick, and James Miller. 2007. "P3P Adoption on e-Commerce Web Sites: A Survey and Analysis." *IEEE Internet Computing* 11 (2): 65–71.

BITAG. 2016. "Internet of Things (IoT) Security and Privacy Recommendations." BITAG Broadband Internet Technical Advisory Group, November 2016. http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf.

Blank, Grant, Gillian Bolsover, and Elizabeth Dubois. 2014. "A New Privacy Paradox: Young People and Privacy on Social Network Sites." American Sociological Association Annual Meeting, San Francisco, CA. Accessed July 4, 2017. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2479938.

Bojanova, Irena, George Hurlburt, and Jeffrey Voas. 2014. "Imagineering an Internet of Anything." *Computer* 47 (6): 72–77. doi:10.1109/MC.2014.150.

British Land. 2017. "Smart Offices | British Land – The Office Agenda." Accessed July 4, 2017. http://officeagenda.britishland.com/smart-offices.

Bui, Nicola, and Michele Zorzi. 2011. "Health Care Applications: A Solution Based on the Internet of Things." Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, Barcelona, Spain, October 26–29, 1–5. ACM.

Buxmann, Peter, Thomas Hess, and Rainer Ruggaber. 2011. "Internet of Services." *Business & Information Systems Engineering* 1 (5): 341–342.

Cavalry. 2014. "Five Star Automotive Cyber Safety Framework." I Am The Cavalry, August 2014. Accessed July 4, 2017. https://iamthecavalry.org/5star.

Cavalry. 2016. "Hippocratic Oath for Connected Medical Devices." I Am The Cavalry, January 2016. Accessed July 4, 2017. https://iamthecavalry.org/oath.

Cavusoglu, Hasan, Huseyin Cavusoglu, and Jun Zhang. 2008. "Security Patch Management: Share the Burden or Share the Damage?." *Management Science* 54 (4): 657–670.
Cerf, Vinton G. 2015. "Access Control and the Internet of Things." *IEEE Internet Computing 19* (5): 96–c3. doi:10.1109/MIC.2015.108.
Cha, Inhyok, Yogendra Shah, Andreas U. Schmidt, Andreas Leicher, and Michael Victor Meyerstein. 2009. "Trust in M2M Communication." *IEEE Vehicular Technology Magazine* 4 (3): 69–75.
Chaudron, S., R. Di Gioia, M. Gemo, D. Holloway, J. Marsh, G. Mascheroni, J. Peter, and D. Yamada-Rice. 2017. "Kaleidoscope on the Internet of Toys - Safety, Security, Privacy and Societal Insights." EUR 28397 EN. doi:10.2788/05383.
Checkoway, S., D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. 2011. "Comprehensive Experimental Analyses of Automotive Attack Surfaces." 2011 USENIX Security Symposium, San Francisco, CA, August 8–11, 77–92.
Chen, Xian-Yi, and Jin Zhi-Gang. 2012. "Research on Key Technology and Applications for Internet of Things." *Physics Procedia* 33: 561–566.
Cherkaoui, A., L. Bossuet, and L. Seitz. 2014. "New Paradigms for Access Control in Constrained Environments." 9th International Symposium on Reconfigurable and Communication-Centric Systems-on-Chip (ReCoSoC), Montpellier, France, May 26–28, 1–4.
Cranor, Lorrie Faith, Serge Egelman, Steve Sheng, Aleecia M. McDonald, and Abdur Chowdhury. 2008. "P3P Deployment on Websites." *Electronic Commerce Research and Applications* 7 (3): 274–293.
Da Xu, L., W. He, and S. Li. 2014. "Internet of Things in Industries: A Survey." *IEEE Transactions on Industrial Informatics* 10 (4): 2233–2243.
DECC (Department of Energy & Climate Change). 2014. "Smart Grid Vision and Routemap Smart Grid Forum." *Smart Grid Forum*, February. doi:URN 14D/056.
DHS. 2016. "US Department of Homeland Security: Strategic Principles for Securing the Internet of Things (IoT)." November 2016. Accessed July 4, 2017. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf.
Dobbins, Danielle L. 2015. "Analysis of Security Concerns and Privacy Risks of Children's Smart Toys." PhD diss., Washington University St. Louis, St. Louis, MO.
Dohr, Angelika, Robert Modre-Opsrian, Mario Drobics, Dieter Hayn, and Günter Schreier. 2010. "The Internet of Things for Ambient Assisted Living." Seventh International Conference on Information Technology: New Generations (ITNG), Las Vegas, USA, April 12–14, 804–809, IEEE.
Doukas, Charalampos, Ilias Maglogiannis, Vassiliki Koufi, Flora Malamateniou, and George Vassilacopoulos. 2012. "Enabling Data Protection Through PKI Encryption in IoT m-Health Devices." IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE), Larnaca, Cyprus, November 11–13, 25–29. IEEE.
Elliott, Chris. 2014. "Elliott Review Into the Integrity and Assurance of Food Supply Networks-Final Report: A National Food Crime Prevention Framework." Department for Environment, Food & Rural Affairs Food Standards Agency.
eMarketer. 2016. "Internet of Things Is Changing How Media and Entertainment Companies Operate." Accessed July 4, 2017. https://www.emarketer.com/Article/Internet-of-Things-Changing-How-Media-Entertainment-Companies-Operate/1013545.
Faezipour, Miad, Mehrdad Nourani, Adnan Saeed, and Sateesh Addepalli. 2012. "Progress and Challenges in Intelligent Vehicle Area Networks." *Communications of the ACM* 55 (2): 90–100. doi:10.1145/2076450.2076470.
Farooq, M. U., Muhammad Waseem, Sadia Mazhar, Anjum Khairi, and Talha Kamal. 2015. "A Review on Internet of Things (IoT)." *International Journal of Computer Applications* 113 (1): 1–7.
Fedorov, Aleksandr, Egor Goloschchapov, Oleg Ipatov, Vyacheslav Potekhin, Viacheslav Shkodyrev, and Sergey Zobnin. 2015. "Aspects of Smart Manufacturing Via Agent-Based Approach." *Procedia Engineering* 100: 1572–1581. doi:10.1016/j.proeng.2015.01.530.
Ferraiolo, David, Janet Cugini, and D. Richard Kuhn. 1995. "Role-based Access Control (RBAC): Features and Motivations." Proceedings of 11th annual Computer Security Application Conference, New Orleans, LA, December 11–15, 241–248.

Feruza, Y. Sattarova, and Tao-hoon Kim. 2007. "IT Security Review: Privacy, Protection, Access Control, Assurance and System Security." *International Journal of Multimedia and Ubiquitous Engineering* 2 (2): 17–32.

Garcia-Morchon, Oscar, Sye Loong Keoh, Sandeep Kumar, Pedro Moreno-Sanchez, Francisco Vidal-Meca, and Jan Henrik Ziegeldorf. 2013. "Securing the IP-based Internet of Things with HIP and DTLS." Proceedings of the sixth ACM conference on Security and Privacy in Wireless and Mobile Networks, Budapest, Hungary, April 17–19, 119–1240. ACM.

General Data Protection Regulation 2016/679. European Union. 2016. http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.

Gerla, Mario, Eun-Kyu Lee, Giovanni Pau, and Uichin Lee. 2014. "Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds." 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, March 6–8, 12 (9): 241–246.

Gessner, Dennis, Alexis Olivereau, Alexander Salinas Segura, and Alexandru Serbanati. 2012. "Trustworthy Infrastructure Services for a Secure and Privacy-Respecting Internet of Things." IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Liverpool, England, June 25–27, 998–1003.

Greveler, Ulrich, Peter Glösekötterz, Benjamin Justusy, and Dennis Loehr. 2012. "Multimedia Content Identification Through Smart Meter Power Usage Profiles." Proceedings of the International Conference on Information and Knowledge Engineering (IKE), Las Vegas, USA, July 16–19.

GSMA. 2016a. "IoT Security Guidelines Overview Document." GSMA Association. Accessed July 4, 2017. https://www.gsma.com/iot/wp-content/uploads/2017/04/CLP.11-v1.1-Overview.pdf.

GSMA. 2016b. "IoT Security Guidelines for IoT Service Ecosystem." GSMA Association. Accessed July 4, 2017. https://www.gsma.com/iot/wp-content/uploads/2017/04/CLP.12-v1.1-Service-Ecosystems.pdf.

GSMA. 2016c. "IoT Security Guidelines Endpoint Ecosystem." GSMA Association. Accessed July 4, 2017. https://www.gsma.com/iot/wp-content/uploads/2017/04/CLP.13-v1.1-Endpoint.pdf.

GSMA. 2016d. "IoT Security Guidelines for Network Operators." GSMA Association. Accessed July 4, 2017. https://www.gsma.com/iot/wp-content/uploads/2017/04/CLP.14-v1.1-Network-Operators.pdf.

Guajardo, J., S. S. Kumar, and G. J. Schrijen. 2007. "Physical Unclonable Functions and Public-Key Crypto for FPGA IP Protection." Proceedings of International Conference on Field Programmable Logic and Applications, Amsterdam, Netherlands, August 27–29, 189–195.

Gusmeroli, Sergio, Salvatore Piccione, and Domenico Rotondi. 2013. "A Capability-Based Security Approach to Manage Access Control in the Internet of Things." *Mathematical and Computer Modelling* 58 (5–6): 1189–1205.

Healy, Michael, Thomas Newe, and Elfed Lewis. 2009. "Security for Wireless Sensor Networks: A Review." IEEE Sensors Applications Symposium, New Orleans, LA, February 17–19, 80–85.

Heer, T., O. Garcia-Morchon, R. Hummen, S. L. K eoh, S. S. Kumar, and K. Wehrle. 2011. "Security Challenges in the IP-based Internet of Things." *Wireless Personal Communications* 61 (3): 527–542.

Henze, Martin, Lars Hermerschmidt, Daniel Kerpen, Roger Häußling, Bernhard Rumpe, and Klaus Wehrle. 2016. "A Comprehensive Approach to Privacy in the Cloud-Based Internet of Things." *Future Generation Computer Systems* 56: 701–718.

Hu, Chih-Lin, Hung-Tsung Huang, Cheng-Lung Lin, Nguyen Huu Minh Anh, Yi-Yu Su, and Pin-Chuan Liu. 2013. "Design and Implementation of Media Content Sharing Services in Home-based IoT Networks." IEEE International Conference on Parallel and Distributed Systems (ICPADS), Seoul, Korea, December 15–18, 605–610.

IBM Watson Foundations. 2015. "Maximize Insight, Ensure Trust and Improve IT Economics – United States." Accessed July 4, 2017. https://www.ibm.com/big-data/us/en/big-data-and-analytics/it-economics.html.

ICO. 2017. "GDPR Consent Guidance for Consultation." Accessed July 4, 2017. https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf.

IEEE. 2014. "Special Report: The Internet of Things." Accessed July 4, 2017. http://theinstitute.ieee.org/static/special-report-the-internet-of-things.

IHS Markit. 2016. "Rapid Expansion Projected for Smart Home Devices." Accessed July 4, 2017. http://news.ihsmarkit.com/press-release/technology/rapid-expansion-projected-smart-home-devices-ihs-markit-says.

INFSO DG 2008. "Internet of Things in 2020: A Roadmap for the Future." INFSO D. 4 Networked Enterprise & RFID, INFSO G. 2 Micro & Nanosystems in Co-operation with RFID Working Group of the European Technology Platform on Smart Systems Integration (EPOSS). European Commission, Brussels, Belgium, Tech. Rep. (ver. 3).

Islam, S. M. Riazul, Daehan Kwak, Humaun Kabir, Mahmud Hossain, and Kyung-Sup Kwak. 2015. "The Internet of Things for Health Care: A Comprehensive Survey." *IEEE Access* 3: 678–708. doi:10.1109/ACCESS.2015.2437951.

Jøsang, Audun, Lothar Fritsch, and Tobias Mahler. 2010. "Privacy Policy Referencing." International Conference on Trust, Privacy and Security in Digital Business, Bilbao, Spain, August 30–31, 129–140.

Karnouskos, Stamatis. 2010. "The Cooperative Internet of Things Enabled Smart Grid." Proceedings of the 14th IEEE International Symposium on Consumer Electronics, Braunschweig, Germany, June 7–10.

Kasem-Madani, Saffija, and Michael Meier. 2015. "Security and Privacy Policy Languages: A Survey, Categorization and Gap Identification." arXiv preprint arXiv:1512.00201.

Kechiche, S. 2015. "Cellular M2M Forecasts: Unlocking Growth". Technical Report, GSMA Intelligence, February 2015. Accessed July 4, 2017. https://www.gsmaintelligence.com/research/?file=9c1e1fdff645386942d758185ceed941&download.

Koscher, Karl, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, et al. 2010. "Experimental Security Analysis of a Modern Automobile." Proceedings of the 2010 IEEE Symposium on Security and Privacy, May 16–19, 447–462. Washington, DC: IEEE Computer Society.

Lee, In, and Kyoochun Lee. 2015. "The Internet of Things (IoT): Applications, Investments, and Challenges for Enterprises." *Business Horizons* 58 (4): 431–440.

Li, Shancang, Li Da Xu, and Shanshan Zhao. 2015. "The Internet of Things: A Survey." *Information Systems Frontiers* 17 (2): 243–259.

Li, L., H. Xiaoguang, C. Ke, and H. Ketai. 2011. "The Applications of WiFi-Based Wireless Sensor Network in Internet of Things and Smart Grid." Paper presented at the proceedings of the 6th IEEE conference on industrial electronics and applications, Beijing, China, June 21–23, 789–793.

Liang, Gaoqi, Steven R. Weller, Junhua Zhao, Fengji Luo, and Zhao Yang Dong. 2017. "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks." *IEEE Transactions on Power Systems* 32 (4): 3317–3318.

Libelium. 2015. "50 Sensor Applications for a Smarter World." Accessed July 4, 2017. http://www.libelium.com/resources/top_50_iot_sensor_applications_ranking/.

Macaulay, James, Lauren Buckalew, and Gina Chung. 2015. "Internet of Things in Logistics." *DHL Trend Research* 1 (1): 1–27.

Machina Research. 2015. "Global M2M Market to Grow to 27 Billion Devices, Generating USD1.6 Trillion Revenue in 2024." Accessed July 4, 2017. https://machinaresearch.com/news/global-m2m-market-to-grow-to-27-billion-devices-generating-usd16-trillion-revenue-in-2024/.

Maglaras, Leandros A., Ali H. Al-Bayatti, Ying He, Isabel Wagner, and Helge Janicke. 2016. "Social Internet of Vehicles for Smart Cities." *Journal of Sensor and Actuator Networks* 5 (1): 3.

Mahalle, Parikshit N., Bayu Anggorojati, Neeli R. Prasad, and Ramjee Prasad. 2013. "Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things." *Journal of Cyber Security* 1 (4): 309–348.

Mahalle, Parikshit, Sachin Babar, Neeli R. Prasad, and Ramjee Prasad. 2010. "Identity Management Framework Towards Internet of Things (IoT): Roadmap and Key Challenges." In *Recent Trends in Network Security and Applications*, edited by N. Meghanathan, S. Boumerdassi, N. Chaki, and D. Nagamalai, 430–439. Berlin: Springer.

Maiti, Abhranil, Inyoung Kim, and Patrick Schaumont. 2012. "A Robust Physical Unclonable Function with Enhanced Challenge-Response Set." *IEEE Transactions on Information Forensics and Security* 7 (1): 333–345.

Maiti, Abhranil, and Patrick Schaumont. 2011. "Improved Ring Oscillator PUF: An FPGA-Friendly Secure Primitive." *Journal of Cryptology* 24 (2): 375–397.
Malina, Lukas, Jan Hajny, Radek Fujdiak, and Jiri Hosek. 2016. "On Perspective of Security and Privacy-Preserving Solutions in the Internet of Things." *Computer Networks* 102: 83–95. doi:10.1016/j.comnet.2016.03.011.
Mansfield-Devine, Steve. 2016. "Securing the Internet of Things." *Computer Fraud & Security* 44 (4): 51–58.
Marin, Eduard, Dave Singelée, Flavio D. Garcia, Tom Chothia, Rik Willems, and Bart Preneel. 2016. "On the Security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them." ACSAC '16 Proceedings of the 32nd Annual Conference on Computer Security Applications, Los Angeles, CA, December 5–8, 226–236. ACM.
Martin, Chase. 2016. "Media and Entertainment Meet the Internet of Things." Accessed July 4, 2017. https://www.mediapost.com/publications/article/278682/media-and-entertainment-meet-the-internet-of-thing.html.
Meola, Andrew. 2016. "Automotive Industry Trends: IoT Connected Smart Cars & Vehicles – Business Insider." Accessed July 4, 2017. http://uk.businessinsider.com/internet-of-things-connected-smart-cars-2016-10?r=US&IR=T.
Minerva, R., A. Biru, and D. Rotondi. 2015. "Towards a Definition of the Internet of Things (IoT)." IEEE Internet Initiative, Torino, Italy, 1.
Miorandi, Daniele, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac. 2012. "Internet of Things: Vision, Applications and Research Challenges." *Ad Hoc Networks* 10 (7): 1497–1516. doi:10.1016/j.adhoc.2012.02.016.
Misra, Sridipta, Muthucumaru Maheswaran, and Salman Hashmi. 2016. *Security Challenges and Approaches in Internet of Things*. Springer Briefs in Electrical and Computer Engineering. Cham: Springer.
Montenegro, G., N. Kushalnagar, J. Hui, and D. Culler. 2007. "Transmission of IPv6 Packets over IEEE 802.15. 4 Networks" (No. RFC 4944).
Morrish, J. 2014. "Business Models for Machine-to-Machine (M2M) Communications." In *Machine-to-Machine (M2M) Communications: Architecture, Performance and Applications*, edited by Carles Anton-Haro and Mischa Dohler, 339–353. Oxford: Woodhead Publishing.
Mulligan, Geoff. 2007. "The 6LoWPAN Architecture." EmNets '07 proceedings of the 4th workshop on Embedded Networked Sensors, Cork, Ireland, June 25–26, 78–82.
Nelson, B. 2016. "Children's Connected Toys: Data Security and Privacy Concerns." United States Congress Senate Committee on Commerce, Science, and Transportation, December 14. Accessed July 4, 2017. https://www.hsdl.org/?view&did=797394.
Nordrum, Amy. 2016. "Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated." *IEEE Spectrum*, August 18. Accessed July 4, 2017. http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated.
Parker, Donn B. 1998. *Fighting Computer Crime: A New Framework for Protecting Information*. New York: Wiley.
Peppet, Scott R. 2014. "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent." *Texas Law Revew* 93: 85.
Perera, Charith, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. 2014. "Context Aware Computing for the Internet of Things: A Survey." *IEEE Communications Surveys & Tutorials* 16 (1): 414–454.
Phillips, Ted, Tom Karygiannis, and Rick Huhn. 2005. "Security Standards for the RFID Market." *IEEE Security and Privacy Magazine* 3 (6): 85–89.
Phull, Suku. 2012. "Intelligent Transport Systems in the UK." *World Scientific*, September. Accessed July 4, 2017. https://ec.europa.eu/transport/sites/transport/files/themes/its/road/action_plan/doc/2012-united-kingdom-its-5-year-plan-2012_en.pdf.
Rainie, Lee, Sara Kiesler, Ruogu Kang, Mary Madden, Maeve Duggan, Stephanie Brown, and Laura Dabbish. 2013. "Anonymity, Privacy, and Security Online." *Pew Research Center*, September 5.
Reay, Ian K., Patricia Beatty, Scott Dick, and James Miller. 2007. "A Survey and Analysis of the P3P Protocol's Agents, Adoption, Maintenance, and Future." *IEEE Transactions on Dependable and Secure Computing* 4 (2): 151–164.

Reay, Ian, Scott Dick, and James Miller. 2009. "A Large-Scale Empirical Study of P3P Privacy Policies: Stated Actions vs. Legal Obligations." *ACM Transactions on the Web (TWEB)* 3 (2): 6.
Riahi, Arbia, Yacine Challal, Enrico Natalizio, Zied Chtourou, and Abdelmadjid Bouabdallah. 2013. "A Systemic Approach for IoT Security." IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), Cambridge, MA, May 20–23, 351–355. doi:10.1109/DCOSS.2013.78.
Roman, Rodrigo, Pablo Najera, and Javier Lopez. 2011. "'Securing the Internet of Things (IoT)'." *IEEE Computer* 44: 51–58. doi:10.1109/MC.2011.291.
Rose, Karen, Scott Eldridge, and Lyman Chapin. 2015. "The Internet of Things: An Overview." *The Internet Society (ISOC)*, October, 1–50.
Sadeghi, Ahmad-Reza, Christian Wachsmann, and Michael Waidner. 2015. "Security and Privacy Challenges in Industrial Internet of Things." 52nd ACM/EDAC/IEEE Design Automation Conference, San Francisco, CA, June 8–10. New York: ACM Press, 1–6.
Sarma, Amardeo C., and João Girão. 2009. "Identities in the Future Internet of Things." *Wireless Personal Communications* 49 (3): 353–363.
Sicari, Sabrina, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. 2015. "Security, Privacy and Trust in Internet of Things: The Road Ahead." *Computer Networks* 76: 146–164.
Smith, Daniel, Scott Lyle, Al Berry, Nicola Manning, Mohamed Zaki, and Andy Neely. 2015. *Internet of Animal Health Things (IoAHT) Opportunities and Challenges*. University of Cambridge. Accessed July 4, 2017. http://cambridgeservicealliance.eng.cam.ac.uk/resources/Downloads/MonthlyPapers/2015JulyCaseStudyIoAHT_HQP.pdf.
Stachel, Joshua R., Ervin Sejdic, Ajay Ogirala, and Marlin H. Mickle. 2013. "The Impact of the Internet of Things on Implanted Medical Devices Including Pacemakers, and ICDs." IEEE International Instrumentation and Measurement Technology Conference, Minneapolis, MN, May 6–9, 839–844.
Stankovic, John A. 2014. "Research Directions for the Internet of Things." *IEEE Internet of Things Journal* 1 (1): 3–9.
Sterbenz, James P. G., David Hutchison, Egemen K. Çetinkaya, Abdul Jabbar, Justin P. Rohrer, Marcus Schöller, and Paul Smith. 2010. "Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines." *Computer Networks* 54 (8): 1245–1265.
Storm, Darlene. 2015. "MEDJACK: Hackers Hijacking Medical Devices to Create Backdoors in Hospital Networks." *Computerworld*, June 8.
Suh, G. Edward, and Srinivas Devadas. 2007. "Physical Unclonable Functions for Device Authentication and Secret Key Generation." ACM proceedings of the 44th Annual Design Automation Conference, Yokohama, Japan, January 23–26, 9–14.
Sun, Chunling. 2012. "Application of RFID Technology for Logistics on Internet of Things." *AASRI Procedia* 1: 106–111.
Suo, Hui, Jiafu Wan, Caifeng Zou, and Jianqi Liu. 2012. "Security in the Internet of Things: A Review." *IEEE International Conference Computer Science and Electronics Engineering (ICCSEE)* 3: 648–651.
Taddeo, M., and L. Floridi. 2011. "The Case for E-Trust." *Ethics and Information Technology* 13 (1): 1–3.
Thoben, Klaus-Dieter, Stefan Wiesner, and Thorsten Wuest. 2017. "'Industrie 4.0' and Smart Manufacturing – A Review of Research Issues and Application Examples." *International Journal of Automation Technology* 11 (1): 4–16. doi:10.20965/ijat.2017.p0004.
Tuyls, Pim, and Boris Škorić. 2007. "Strong Authentication with Physical Unclonable Functions." In *Security, Privacy, and Trust in Modern Data Management*, edited by Milan Petković and Willem Jonker, 133–148. Berlin: Springer-Verlag.
Uckelmann, Dieter, Mark Harrison, and Florian Michahelles. 2011. "An Architectural Approach Towards the Future Internet of Things." In *Architecting the Internet of Things*, edited by Dieter Uckelmann, Mark Harrison, and Florian Michahelles, 1–24. Berlin: Springer.
Vermesan, Ovidiu, Peter Friess, Patrick Guillemin, Sergio Gusmeroli, Harald Sundmaeker, Alessandro Bassi, Ignacio Soler Jubert, et al. 2011. "Internet of Things Strategic Research Roadmap." *Internet of Things-Global Technological and Societal Trends* 1: 9–52. Accessed July 4, 2017. http://internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2011.pdf.
Vetter, R. J. 1995. "Internet Kiosk-Computer-Controlled Devices Reach the Internet." *Computer* 28 (12): 66–67.

Wang, Y., and A. Kobsa. 2009. "Privacy-enhancing Technologies." In *Handbook of Research on Social and Organizational Liabilities in Information Security*, edited by M. Gupta and R. Sharman, 203–227. Hershey, PA: IGI Global.

Weber, R. H. 2010. "Internet of Things – New Security and Privacy Challenges." *Computer Law & Security Review* 26 (1): 23–30.

Whitmore, Andrew, Anurag Agarwal, and Li Da Xu. 2015. "The Internet of Things - A Survey of Topics and Trends." *Information Systems Frontiers* 17 (2): 261–274.

Yan, Zheng, and Silke Holtmanns. 2008. "Trust Modeling and Management: From Social Trust to Digital Trust." In *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions*, edited by Ramesh Subramanian, 290–323. Hershey, PA: IGI Global.

Yan, Zheng, Peng Zhang, and Athanasios V. Vasilakos. 2014. "A Survey on Trust Management for Internet of Things." *Journal of Network and Computer Applications* 42: 120–134. doi:10.1016/j.jnca.2014.01.014.

Zanella, Andrea, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi. 2014. "Internet of Things for Smart Cities." *IEEE Internet of Things Journal* 1 (1): 22–32. doi:10.1109/JIOT.2014.2306328.

Ziegeldorf, Jan Henrik, Oscar Garcia Morchon, and Klaus Wehrle. 2014. "Privacy in the Internet of Things: Threats and Challenges." *Security and Communication Networks* 7 (12): 2728–2742.