Please cite as: Kevin Curran (2018) *Security and the Internet of Things* in Cyber Security: Law & Guidance Handbook, Bloomsbury Publishers, London, UK. pp: 371-382, ISBN: 978-1-52650-586-6

Security Concerns with the Internet of Things

Kevin Curran
Professor in Cyber Security at Ulster University, Northern Ireland

Abstract

The Internet of Things (IoT) also known as Web of Things (WoT) is a concept where everyday devices - home appliances, sensors, monitoring devices - can be accessed through the internet using well known technologies such as URLs and HTTP requests. This chapter highlights some of the aspects of the Internet of Things which are causing global security issues and suggests some steps which can be taken to address these risks.

1. Introduction

The Internet of Things (IoT) will offer the ability for consumers to interact with nearly every appliance and device they own (McKeever et al., 2015). For example, your refrigerator will let you know when you are running low on cheese and your dishwasher will inform you when it's ready to be emptied. It is possible that consumers will be receiving more text messages from their devices than human beings soon. We are seeing elements of the IoT in the marketplace already, with home automation having a strong consumer pull, from controlling the lights and temperature to closing the garage door while away from the home. In a more comprehensive way, IoT transforms real world objects into smart objects and connects them through the Internet (Fathi & Curran, 2017). In contrast with the current Internet, IoT depends on a dynamic architecture where physical objects with embedded sensors will communicate with an e-infrastructure (i.e. a cloud) to send and analyse data using the Internet Protocol. IoT envisions a future in which digital and physical entities can be linked, through their unique identifier and by means of appropriate information and communication technologies (Curran & Curran, 2014). However, like any new technology or idea, there are kinks that need to be worked out. If IoT is campaigning to run nearly every aspect of our digital lives, considerations need to be made to ensure a seamless and safe introduction. Security, standards and overburdening the network are just some of the requirements that need to be focused on before implementing for mass adoption in the modern business place (IEEE, 2012a; IEEE, 2012b).

Being connected to the Internet of Things in the very near future is going to happen seamlessly through modern technologies such as connected home appliances and wearables (Carlin & Curran, 2013). For instance, the Mimo baby monitor is a body suit that monitors a baby's body temperature, motion, and breathing patterns. Sensors use Bluetooth wireless communication to relay this data to a base station, which then transmits it to the Internet to be analyzed by the company's sleep analysis software (Rodriguez McRobbie, 2014). Lively is a system composed of activity sensors placed on objects around the home that monitors the daily behaviour of an individual living alone. For example, sensors may be placed on a refrigerator door, a pill box, and car keys to collect data on an individual's eating, medication, and sleep habits. Shockbox[1] is a small, flexible sensor that fits inside of a sports helmet and monitors the history of head impacts athletes sustain. Shockbox sensors communicate using Bluetooth to immediately alert parents, coaches, and trainers in the event of a concussion-level impact. The Nuubo Smart Shirt[2] is a sensor-equipped shirt that monitors a patient's vital signs and movement. The sensors in the shirt can take regular measures on items such as heart rate, blood

[1] http://www.theshockbox.com/
[2] https://www.nuubo.com/

pressure, and body temperature. In addition, it can conduct an electrocardiogram (ECG). The shirt sends data wirelessly to a server for data analysis where, for example, software can detect anomalies in the ECG. The CardioMEMS Heart Sensor[3] is an implantable medical device for monitoring heart failure. The device, which is about the size of a paper clip, is implanted into a patient's pulmonary artery using a minimally-invasive technique and measures pulmonary arterial pressure. Data from the device is collected wirelessly and transmitted to a central database for the patient's health care providers to review. The "always ready" capability leads to a new form of synergy between human and computer, characterized by long-term adaptation through constancy of user-interface. The arrival of wearable devices has been made possible by advancements in miniaturising electronics and in part to advances in battery technologies. Connecting these devices to the Internet of Things will usher in a new world of truly big data (Smedley, 2016). Consumer electronics are benefitting from the Internet of Things. Samsung Electronics president, Boo-Keun Yoon has said that 90 per cent of the company's household appliances (as well as its TVs, computers, smartphones and smartwatches) will be IoT devices within two years, and that the entire tech industry will fall into line within five (Tibkem, 2015). Some estimations are that the worldwide market for Internet of Things solutions will grow to $7.1 trillion in 2020. Like many technologies however, there are negative as well as positive aspects to consider.

Positive aspects of IoT are demonstrated by environmental industries which are using multifaceted IoT solutions to protect our environment (Deak et al., 2013). These include clean water, air pollution, landfill waste, and deforestation. Sensor-enabled devices are already helping monitor the environmental impact of cities, collect details about sewers, air quality, and garbage. In rural areas, sensor-enabled devices can monitor woods, rivers, lakes, and our oceans. Many environmental trends are so complex, that they are difficult to conceptualize, but collecting data is the first step towards understanding, and ultimately reducing, the environmental impact of human activity (Carlin & Curran, 2014). WaterBee[4] is a smart irrigation system that collects data on soil content and other environmental factors from a network of wireless sensors to reduce water waste. The system analyses the data it collects to selectively water different plots of land based on need. Waterbee can be used for a variety of commercial applications, including on farms, vineyards, and golf courses. Smart irrigation systems save energy, water, and money (Schneps-Schneppe et al., 2012). Using a prototype, fourteen sites in Europe were able to reduce their water usage on average by 40 percent. Z-Trap helps prevent crop damage by using pheromones to trap insects and then compile data on the number of different types of insects in the trap. Z-Trap wirelessly transmits the data, including its GPS coordinates, allowing farmers to view a map of the types of insects that have been detected. Construction is also benefitting from the Internet of Things. For instance, wireless bridge sensors can help reduce this risk by monitoring all aspects of a bridge's health, such as vibration, pressure, humidity, and temperature. The U.S. Geological Survey Advanced National Seismic System uses accelerometers and real-time data analysis to monitor the structural health of buildings in earthquake prone regions. Sensors detect the degree of the building's movement, the speed that seismic waves travel through the building, and how the frame of the building changes (Gubbi et al., 2013).

There are however quite a few risks. Technical challenges include government regulation with regards spectrum allocation, security, battery issues, costs and privacy. One of the successes of the UK IoT has been the introduction of 'smart meters'. These are network connected meters which 'broadcast' our power usage to the power company. There is however a real possibility that unscrupulous individuals can commit a crime by manipulating the data captured by the meter. A hacker for instance could compromise a smart meter to find out about a home owners' peaks of use to learn when they are likely to be out. On a larger scale however, there is a threat whereby smart meters which are connected to smart grids could be attacked leading to complete failure of the system.

[3] https://www.sjm.com

[4] http://waterbee-da.iris.cat/

Manufacturers of devices which will contribute to the Internet of Things need to consider the correct forms of cryptographic algorithms and modes needed for IoT devices. There is an international ISO/IEC 29192 standard which was devised to implement lightweight cryptography on constrained devices. There was a need for this as many IoT devices have a limited memory size, limited battery life along with restricted processors. Traditional 'heavy' cryptography is difficult to deploy on a typical sensor hence the deployment of many insecure IoT devices. Regulations for the Internet of Things need to address issues of 'minimum specifications' for IOT devices.

Ultimately, we can expect to see an explosion in the amount of data collected. There is much value in that data, but one needs to be trained and have a good knowledge of Big Data (Zaslavsky, 2013). Big data is a term for large data sets where the traditional data processing approaches simply do not work due to their complexity. These data sets however possess potential to reveal business trends, identification of diseases, combat crime and much more. There is a great need for people with Business Analytics skills to mine big data. The role of a business analyst is to aggregate data to work out how an organization can leverage data to operate more efficiently. Predictive analytics is one of the tools which can deal with the sheer complexity of a global Internet of Things. We next look at how implementing security in the Internet of Things differs than traditional methods of rolling out security mechanisms.

2. How organisations can secure IoT

Hackers attempting to attack IoT device typically try to either take control of the device, steal information, or disrupt the service it is offering. A rudimentary way to prevent these attacks is to prevent communication with the devices they are trying to hack with a firewall and an Intrusion Detection & Prevention System (IDPS). Here a firewall blocks that should not be passing through. The IDPS monitors the system and network to detect, block, and report suspicious events. The problem however to regular IT security is that firewalls and antivirus programs require a lot of storage space and sufficient processing power to run but many IoT devices are not powerful enough to run these. Therefore, IoT security is different in that we must recognise that IoT devices are primarily embedded dedicated computer systems - and quite limited at that. They are often single purpose devices performing specific functions within a wider more complex system e.g. Light bulb, TVs, pacemakers, plant watering control systems, kettles. Providing only limited functions allows them to be lean and cheap.

Here then, the security mechanisms must be equally specialised and aimed at protecting against more targeted attacks which are quite often unique to the functionality of that device. Adopting security support ecosystems such as large databases of malware signatures is unlikely to find adoption or be implementable on these devices. A more practical solution is to enforce rules-based filtering so that for instance white-list rules allows communications only from specific authorised devices. Firewall policies like this allow a much-reduced rule set to be adopted. IoT manufacturers such as Intel, McAfee and Zilog are building these embedded security technology practices into the hardware and software for IoT devices. Unfortunately, there are many older IoT devices which are unable to be updated to support these policies in their software so in those cases, an intermediate firewall needs to be added to the network to defend those devices against outside attacks. Firewalls only prevent a subset of attacks however and other problems such as eavesdropping require additional mechanisms in place.

Organisations need to ensure they deploy IoT devices with sufficient security policies in place such as firewalls and intrusion detection & prevention systems, but they also need to ensure they cater for the confidentiality of their customers data. This is where encryption plays a core role. All devices need strong passwords. It is also good practice to enforce certificate-based authentication which identifies communicating individuals and authorised devices. This is currently used in POS terminals, petrol pumps, and ATMs. Device management agents can also highlight failed access attempts and attempted denial-of-service attacks. All non-IoT devices must also be patched and kept malware free. These could as likely be the pivot point for infecting IoT devices. Biometric authentication methods are increasingly being offered to add another layer.

Many of the steps in securing IoT activities are like security steps within the larger enterprise system. Organisation do however need to be aware that privacy issues can arise due to their IoT data collection mechanisms which may lead to user profiling and identification of individuals in unforeseen use case scenarios. The greatest care needs to be taken when deploying data collection devices with regards their lifecycle, data collection mechanisms and overall security protocols. It is crucial that information security, privacy and data protection be addressed comprehensively at the design phase. We need to start training our graduates in best practice aggregation and anonymity of data. Yes, collect data which benefits society but we need those who do so to know how to scrub if first from individual identifying information which invades our privacy.

Companies will have to pay more attention to the secure storage of data collected via the Internet of Things as legal repercussions creep in and the increase in data being collected (McBride et al., 2015). This data is generally being stored in the cloud (Zhou et al., 2013). Therefore, all the recommended practices applicable to securing data in the cloud equally applies here. Companies should with large data sets due to the multi-tenant nature of a cloud platform pay extra attention to the data lifecycle phases and ensure that aspects such as data destruction is provided and auditable as part of the service. The fact that any company is allowing confidential datasets to reside outside the company network should lead them to examine how they can robustly protect that data.

Ultimately, it is critical that they implement a layered security strategy regarding cloud services as their data is more exposed than previously. It is critical to get buy in from upper-management. More so than ever, security breaches can greatly affect their reputation. Cybercrime is on the rise therefore we should think about security in terms of process, people and technology. This will involve creating security policies with internal departments, performing audits, implementing physical security control and classifying risk. The rapid rollout of IoT devices and connectivity to external parties has led to increased risks to an organisation's internal assets (Lee & Lee, 2015). Information that is more valuable than ever before is more accessible and easier to divert. Organisations that fail to address the broader security issues that accompany this change will have insufficient controls in place to minimize risks. These risks could lead to significant financial, legal difficulties and reputation risk for these organisations (Mc Kelvey et al., 2014). Appropriate preventive, detective and corrective controls in the form of policies, standards, procedures, organisational structures or software/technology functions and monitoring mechanisms are therefore required to minimise the risks associated with the confidentiality, integrity and availability of information assets within an organisation. These aspects of security should be the underpinnings of any Internet of Things Regulations policy.

There is no established formula for balancing risk with security level and the subsequent investment. However, companies who follow industry standards such as ISO 27001 which is a specification for an information security management system will tangentially balance risk with investment. This standard seeks to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system so adhering to the recommended best practices should ensure at least a minimum outlay in security measures. Of course,

organisations will differ. No one questions that a military organisation will require an equivalent budget (or percentage) to a corner shop but auditing risk should flag the critical weak points and lead to investment in securing those aspects.

3. Industry-wide initiatives for IoT security

There are several industrywide initiatives for IoT security currently (IEEE 2011; IEEE 2012c). It is not an easy task as regulating IoT devices means devising a rule that would be broad enough to cross many sectors and cover all these products. The security expert Bruce Schneier intelligently said that a good starting place would be "minimum security standards, interoperability standards, the ability to issue a software update or patch after a product has hit the market, and even placing code in escrow so that problems can still be managed in case a company goes out of business". It is hard to argue with that. The reason for the delay is simply due to many IoT devices being low-margin products hence the lack of urgency from manufacturers. It would be fair to say that there is no overarching IoT security initiative but rather several standards which address aspects of security that can be applied to the Internet of Things, including IEEE P1363, a standard for public-key cryptography; IEEE P1619 addresses encryption of data on storage devices; IEEE P2600 addresses the security of printers; and IEEE 802.1AE/IEEE 802.1X address media access control security (IEEE, 2013).

The National Institute of Standards and Technology has created a voluntary cybersecurity framework that companies, and organizations can use as a guide to identify and protect against cyber risks. However, it was intended to protect critical infrastructure such as the electricity grid and water treatment plants and does not have specific recommendations for IoT devices. Other security standards for the IoT include the North American Electric Reliability Corp. who have outlined critical infrastructure protection standards to secure the electric grid. The U.S. Food and Drug Administration has a set of guidelines to help product makers better protect patient health and information. The Open Interconnect Consortium comprised of companies such as Cisco and Intel have developed interoperability standards for the IoT which also include security aspects. IEC 62443/ISA99, Industrial Automation and Control System Security Committee has defined procedures for implementing secure industrial automation and control systems. Finally, the International Standards Organization (ISO) has a special Working Group on the Internet of Things and this is important as their security standard ISO 27000 is globally popular (Calder, 2006).

Whilst not a standard, there are also initiatives to increase IoT security such as where Microchip Technology and Amazon.com have created an add-on chip to make devices more secure. Cloud services are a key part of IoT where connected IoT devices rely on large-scale cloud infrastructure but this chain from device to owner and back is a weak link for spoofing attacks (Ksiazak et al., 2015). The AWS-ECC508 provides end-to-end security between the IoT device and the cloud infrastructure by verifying the identity of the AWS cloud service and the IoT device. The identities are based on cryptographic keys which traditionally relied on the original manufacturer to securely generate keys. Now however, the AWS-ECC508 can generate its own keys that Amazon will accept as authentic. It also adopts an “elliptic curve cryptography” algorithm which is more efficient and uses less computing resources and is designed to protect against hardware attacks, such as removing the casing to probe the circuitry. This is a step in the right direction for securing the IoT.

4. Future IoT Innovations

Edge computing is innovative with regards IoT devices. An edge device is anything that provides an entry point to a network so by embracing edge computing for IoT devices, they can more efficiently reduce latency for critical applications, remove dependency on the cloud, and ultimately reduce the network loads from data being generated. Examples would be edge IoT computing devices that rapidly react to alarms by taking autonomous decisions.

The rise of home assistants will continue not just in the form of Amazon echo and Google Home, but voice assistants baked into everyday devices. Many of us are using chatbots already in the form of Apple's Siri, Amazon's Echo and Microsoft's Cortana. For instance, if you ask Siri what the weather will be like for an upcoming event, you are basically chatting to a chatbot more commonly known as a personal assistant. We can expect to see more of these.

Incorporation of machine learning on wearable IoT devices. Deploying intelligent algorithms on IoT devices in healthcare enables self-monitoring of health. It also allows the mining of the data streams to pre-empt future health problems, incorporating flags in order that individuals become aware of possible health problems long before they manifest themselves in the real world. In addition, predictive modelling, can help researchers understand and mitigate the behavioural, genetic and environmental causes of disease. More innovation in this IoT space will see the market for wearables expand.

The blockchain also has an important role to play in IoT in the days ahead. Scaling the Internet of Things will prove difficult using traditional centralised models. There are also inherent security risks in the Internet of Things such as disabling them should they become compromised and become parts of botnets which has become a serious problem already. The Blockchain however with its solid cryptographic foundation offering a decentralized solution which can aid against data tampering thus offering greater assurances for the legitimacy of the data. Blockchain technology could potentially allow billions of connected IoT devices to communicate in a secure yet decentralized ecosystem which also allows consumer data to remain private.

There are already blockchain-based IoT frameworks such as ChainAnchor which includes layers of access to keep out unauthorized devices from the network. IBM Watson IoT Platform enables IoT devices to send data to blockchain ledgers for inclusion in shared transactions with tamper-resistant records. It also validates the transaction through secure contracts. Another blockchain solution from Australian researchers uses a block miner to manage all local network transactions to control communication between home-based IoT devices and the outside world. It can authorise new IoT devices and cut off hacked devices. Telestra is using blockchain to secure smart home IoT ecosystems by storing biometric authentication data to verify identity of people. IBM's Blockchain provide audit trails, accountability, new forms of contracts and speed for IoT devices. They see the benefit of underpinning the IoT with Blockchain as trust, cost reduction and the acceleration of transactions.

5. Future Short-Term Challenges

Security of IoT device remains a challenge (Ksiazak et al., 2018). Compromised IoT devices have been responsible for many large-scale botnets in recent times. Security standards are a key requirement that need to be focused on before implementing for mass adoption in modern life and more accountability for manufacturers with regards roadmaps for updates for any devices they sell.

Good throughput is also a challenge for IOT. Although it is still a concept 5G has some wonderful attributes - not least - conservation of battery life which may transform the IOT in the future. Multiple input multiple output (MiMo) technology is set to be a key part of these efficiency measures. Existing IOT sensors however are not equipped to take advantage of 5G technology. Samsung, Huawei and others are already playing with new 5G technologies and leading the way.

Companies will have to pay more attention to the secure storage of data collected via the Internet of Things as legal repercussions arrive in the form of the EU GDRP. IoT data is generally stored in the cloud, therefore all the recommended practices applicable to securing data in the cloud equally applies here. Companies should with large data sets due to the multi-tenant nature of a cloud platform pay extra attention to the data lifecycle phases and ensure that aspects such as data destruction is provided as part of the service.

To date, only a few IoT manufacturers are considering the correct forms of cryptographic algorithms and modes needed for IoT devices (Curran et al., 2015). There is an international ISO/IEC 29192 standard which was devised to implement lightweight cryptography on constrained devices. There was a need for this as many IoT devices have a limited memory size, limited battery life along with restricted processors. Traditional 'heavy' cryptography is difficult to deploy on a typical sensor hence the deployment of many insecure IoT devices. Severe pressure needs to be placed on IoT manufacturers to implement best practice in securing these devices before they leave the factory. We know the public will be unaware of the need to update their lightbulbs so we in the security industry must force the manufacturers to not make it so easy for the hackers to exploit them. As we have seen lately, we are now all at risk from IoT devices which were thought to be too dumb to cause harm. The opposite is the truth. Unpatched, poorly deployed dumb devices have the power to bring the Internet to its knees.

6. Conclusion

There is an argument for organisations to keep it dumb when it comes to the Internet of Things. A basic rule of thumb in security is that the more devices you have exposed to the internet, then the more exposure you must to being hacked. It simply means that you are more likely to have neglected devices which are not updated and hence more vulnerable. It is crucial that IT departments monitor their networks 24-7, looking for potential intrusions and unusual activity on the network but not many do this and take appropriate actions.

The sheer scale of deployment of these limited-function embedded devices in households and public areas can lead to unique attacks. There is also the worry of the domino effect where if one device becomes 'owned' - it can easily spread to the remainder of the cluster. The privacy issues arise due to the data collection mechanisms which may lead to user profiling and identification of individuals in unforeseen use case scenarios. The utmost care needs to be taken when deploying IoT devices with regards their lifecycle, data collection mechanisms and overall security protocols. We have now seen a major issue with IoT devices due to their implementation of default passwords which are known to hackers in addition to many of these devices have pre-installed unchangeable passwords which is utterly careless on behalf of the manufacturers. The days ahead may see IoT hardware manufacturers being held more accountable for the security of the products they ship and having to ensure any vulnerabilities are patched in a timely acceptable fashion.

References

Botta, A., de Donato, W., Persico, V., Pescapé, A. (2016) Integration of cloud computing and internet of things: a survey, Future Gener. Comput. Syst., 56, pp. 684-700

Calder, A. (2006) Information Security Based on ISO 27001/ISO 17799: A Management Guide Van Haren Publishing 2006

Carlin, S., Curran, K. (2013) An Active Low-Cost Mesh Networking Indoor Tracking System. IoT-SoS 2013 – The Second IEEE WoWMoM Workshop on the Internet of Things: Smart Objects and Services, Madrid, Spain, 4th-7th June 2013

Carlin, S., Curran, K. (2014) An Active Low Cost Mesh Networking Indoor Tracking System. International Journal of Ambient Computing and Intelligence, Vol. 6, No. 1, January-March 2014, pp: 45-79, DOI: 10.4018/ijaci.2014010104

Copie, A., Fortiş, T., Munteanu, V. (2013) Benchmarking cloud databases for the requirements of the internet of things, Information Technology Interfaces (ITI), Proceedings of the ITI 2013 35th International Conference on, IEEE, pp. 77-82

Curran, K., Curran, N. (2014) *Social Networking Analysis.* Big Data and Internet of Things: A Roadmap For Smart Environments, pp: 366-378, DOI: 10.1007/978-3-319-05029-4, ISBN: 978-3-319-05029-4, Springer International Publishing Switzerland 2014

Curran, K., Maynes, V., Harkin, D. (2015) Mobile Device Security. International Journal of Information and Computer Security, Vol. 6, No. 3, January 2015, pp: 55-68, ISSN: 1744-1765

Deak, G., Curran, K., Condell, J., Bessis, N., and Asimakopoulou, E. (2013) *IoT (Internet of Things) and DfPL (Device-free Passive Localisation) in a disaster management scenario.* Simulation Modelling Practice and Theory, Vol. 34, No. 3, pp: 86-96, DOI: 10.1016/j.simpat.2013.03.005, ISSN: 1569-190X, Elsevier Publishing

Fathi, A., Curran, K. (2017) Detection of Spine Curvature using Wireless Sensors. Journal of King Saud University – Science. Vol. 29, No. 4, October 2017, pp: 553-560, Elsevier, ISSN: 1018-3647, DOI: http://dx.doi.org/10/1016/j.jksus.2017.09.014

Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M. (2013) Internet of Things (IoT): a vision, architectural elements, and future directions, Future Gener. Comput. Syst., 29 (2013), pp. 1645-1660

IEEE 802.22 (2011) IEEE Standard for Information Technology--Telecommunications and information exchange between systems Wireless Regional Area Networks (WRAN)--Specific requirements Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands

IEEE 802.15.4f (2012a) IEEE Standard for Local and metropolitan area networks-- Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 2: Active Radio Frequency Identification (RFID) System Physical Layer (PHY)

IEEE 802.15.6 (2012b) IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 15.6: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)used in or around a body

IEEE 802.16 (2012c) IEEE Standard for Air Interface for Broadband Wireless Access Systems

IEEE 802.15.4j (2013) IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs) Amendment: Alternative Physical Layer Extension to support Medical Body Area Network (MBAN) services operating in the 2360-2400 MHz band

Ksiazak, P., Farrelly, W., Curran, K. (2015) A Lightweight Authentication Protocol for Secure Communications between Resource-Limited Devices and Wireless Sensor Networks. International Journal of Information Security and Privacy, Vol. 8, No. 4, pp: 62-102, October-December 2015, DOI: 10.4018/IJISP.2014100104, ISSN: 1930-1650, IGI Global

Ksiazak, P., Farrelly, W., Curran, K. (2018) A Lightweight Authentication Protocol for Secure Communications between Resource-Limited Devices and Wireless Sensor Networks. Security and Privacy Management, Techniques, and Protocols, April 2018, ISSN: 1522555838 IGI Global

Lee, I., Lee, K. (2015) The Internet of Things (IoT): applications, investments, and challenges for enterprises, Bus. Horiz., 58 (2015), pp. 431-440

McBride, B., McKelvey, N., Curran, K. (2015) Security issues with contactless bank cards. Journal of Information, Vol. 1, No. 3, DOI: 10.18488/journal.104/2015.1.3/104.3.53.58, pp: 53-55, 2015

Mc Kelvey, N., Clifton, M., Quigley, C., Curran, K. (2014) Internet Copyright Laws and Digital Industries. International Journal of E-Business Development (IJED), Vol. 3, No. 4, pp: 174-178, ISSN:2225-7411

McKeever, P., McKelvey, N., Curran, K., Subaginy, N. (2015) *The Internet of Things*. Encyclopaedia of Information Science and Technology, 3rd Edition, IGI Global Publishing, USA, 2015, pp: 5777-5784, ISBN: 9781466658882, DOI: 10.4018/978-1-4666-5888-2

Rodriguez McRobbie, L. (2014) Selling Fear - Smart monitors cannot protect babies from SIDS, so what are they for? Slate, February 2014, http://www.slate.com/articles/life/family/2014/02/mimo_and_other_smart_baby_monitors_don_t_protect_from_sids_so_what_are_they.html

Schneps-Schneppe, M., Maximenko, A., Namiot, D., Malov, D. (2012) Wired Smart Home: energy metering, security, and emergency issues, Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2012 4th International Congress on, IEEE (2012), pp. 405-410

Smedley, T. (2016) Wearables for babies: saving lives or instilling fear in parents?, Guardian, May 30th 2016 https://www.theguardian.com/sustainable-business/2016/may/30/wearables-for-babies-saving-lives-or-instilling-fear-in-parents

Tibkem, S. (2015) Samsung, SmartThings and the open door to the smart home (Q&A), CNET, January 12 2015 https://www.cnet.com/g00/news/smartthings-ceo-on-samsung-being-open-apples-homekit-and-more-q-a/

Zaslavsky, A., Perera, C., Georgakopoulos, D. (2013) Sensing as a Service and Big Data arXiv arXiv:1301.0159

Zhou, J., Leppänen, T., Harjula, E., Ylianttila, M., Ojala, T., Yu, C., Jin, H. (2013) Cloudthings: a common architecture for integrating the internet of things with cloud computing, Computer Supported Cooperative Work in Design (CSCWD), 2013 IEEE 17th International Conference on, IEEE (2013), pp. 651-657