Computer Communication & Collaboration (Vol. 3, Issue 4, 2015)
ISSN 2292-1028(Print) 2292-1036(Online)
Submitted on Nov. 21, 2015
(DOIC: 2292-1036-2015-04-002-62)

Personal Information Security and the IoT: The Changing Landscape of Data privacy

Vladlena Benson

Kingston University London, Kingston upon Thames, UK, KT2 7L

E-mail: v.benson@kingston.ac.uk

Abstract: The fast pace of technology innovations are transforming networking paradigm. One of the technologies at the top of the hype-cycle is the Internet of Things(IoT), which connects any object with required identification and appropriate capabilities to be connected to the internet and to one another. The IoT is a truly transformational innovation with the potential to change the way we use wearable devices, smart devices, appliances and services. It offers to take data collection and business intelligence to a previously unimaginable level. This is a ‘sense-making paper’ addressing conceptualisation of individual privacy within the environment, exploiting the IoT innovation. The academic attention is drawn to three dimensions needing further research attention: device and connectivity security; identity, device and data management; and personal privacy in the IoT.

Keywords: Information Security, IoT, Device Connectivity, Enterprise Security

1 Introduction

Millions of enterprises throughout the world and billions of people on the globe lead a digital version of their business activities and personal life online. Anyone in a possession of an internet-connected device (e.g. as simple as digital camera or a music player) contributes to the data in the digital universe. Data is generated by the millions of sensors and communication devices sending and receiving data through online channels. The paradox of data generation is visible when we consider the sources of digital information. While 85% of the digitised information is created by enterprises, over two thirds of data are generated and produced by individual users, such as employees and consumers. We know that the digital universe is doubling in size every two years, we are expecting that the amount of accumulated data will exceed 44 ZB (zettabytes; 1 ZB =1000000 PB) by 2020 [4]. With every embedded system appliance from a refrigerator to 4G enabled cars continuously collecting, communicating, processing information about behaviours, location, habits and preferences, control over personal information [3] has been implicitly taken away from individuals[1].

2 The Next Big IoT Thing

The IoT comprises of connected devices with the capability to automatically manage, monitor, provision and communicate wired or wireless device data over the network. Not only embedded and smart devices and intelligent systems are a part of the network, but the IoT encompasses analytical and integrated capabilities. Therefore, it surpasses the functionality of earlier device –to-device network solution; the nature of IoT takes device connectivity to the next level. However, platforms for device connectivity, application enablement, management, analytics and vertical industry solutions are yet to reach agreed industry standards.

IoT brought about fantastic opportunities for the transformation of the information and communication industry. New business models are formulated as a result of this disruptive technology, which has the potential to enable new value streams for customers, speed time to market and distinctly transform firms' response to customer needs. However, the challenges of device integration, data processing and storage are at the top of the IT sector agenda. In order to make the most of the IoT potential, the IT sector needs to set priorities and address certain imperatives. One of them being the information security in cloud solutions, such as virtual datacentres, public, hybrid and private cloud integration; challenges of cutting-edge analytics required for next generation data processing, storage management technologies, innovation in data access and processing capabilities, automatic tagging and on the fly data analysis require fast pace solutions often leaving security and privacy considerations as an afterthought. This paper highlights the areas of IoT information security which need to be addressed to enable enterprises become more data- and IT-driven.

3 The origins of data in IoT

The entertainment industry led the way to complete digitisation of its service provision, this includes TV and film, ultimately imposing significant demands on media streaming and data storage practices. Current processes in virtualized data centers are challenged by the exponentially increasing volumes of data generated by embedded systems, which include MP3 players, healthcare devices to CCTV cameras and traffic lights. Another growing segment of the digital universe is metadata, - data about data which helps process and identify its owners, such as the additional information in email message metadata. It contains when the email is generated, its origin, type, destination, etc. In the past has been inseparable with the data it identifies. Metadata has now entered its own category and is said to be the fastest expanding.

According to the reports from IDC [6] there are at least forty types of devices generating data in the IoT. They include such long standing micro technologies as the RFID tags and NFC sensors, embedded systems in vehicles and airplanes to particle colliders and supercomputers. However data is only as useful as how well it is processed, i.e. tagged and analysed. The IDC estimates a 10% increase of useful data in seven years; they predict that only about 37% of the digital universe data will be tagged and analysed by 2020.

4 Challenges of the IoT

According to the European commission "the R&D innovation in IoT are around embedded systems, and cyber-physical systems, network technologies, semantic interoperability, operating systems and security and generic enablers". Despite the promise of innovative revenue potential, the IoT presents challenges of its own, these include a lack of universal standards or information security underpinning, the capability to scale globally and an undeveloped ecosystem. From the vendor/supplier perspective, the uniform IoT market and fully realised revenue streams are yet to emerge, each industry and application appear to be isolated. Users, on the other hand, are finding challenges to come to terms to real-time demand of IoT services, while from enterprise viewpoint, issues of managing devices, information, flowing in real-time and in a global workplace may not be widely accepted and regulation challenged.

While the business and individual benefits of the IoT are obvious, the envisaged ecosystem of interconnected devices faces significant challenges of complexity with every device sensing, interacting, and communicating with each other thereby creating innovative services that will bring tangible benefits to the individuals, the economy and the society. At present eight billion smart devices are in human possession, with the IoT making each RFID tag exploitable, the amount of smart objects will grow exponentially in the environment. However, the challenge of diversity and heterogeneity of the variable pool of devices will need to be addressed and the difficulties of resource capabilities, lifespan and communication technologies remain unresolved in current technology architecture. Stemming from that are new issues spanning such domains as: architecture, communication, identification, discovery, data and network management, power and energy storage, security and privacy as highlighted by [11]. It has been acknowledged that existing networking solutions are far from being capable of coping with the unprecedented levels of device connectivity and management, and therefore must be revisited deal with the complex requirements levied by the IoT. Therefore, the need for the development of new intelligent algorithms, ‘fabric’ networking principles and agile services for the IoT has intensified. We therefore draw the academic community attention to the challenges presented by the IoT architecture, connectivity and device heterogeneity and encourage further research efforts in these directions.

5 Security Threats in IoT

As a network of things connected to each other and the internet; the safety of items connected to and the network they communicate to is the objective with IoT security. Each device connected to the IoT is equipped with unique identifiers and are able to automatically communicate data over network. Machine to machine communication systems, home automation, energy grids, car-to-car communication and wearable devices are increasing the volume of data and are vulnerability points in the IoT. Vulnerabilities caused by using passwords which are easy to guess or relying on default passwords on embedded systems which can be easily exploitable. As the IoT is still in its early stages, embedded systems in devices have been oriented to offer new functionality, but security was not thought through at the outset and not built in at the design stage. In order to increase security, things (devices) need to be connected to own network fragment and have other device access restricted. Monitoring of network segments for suspicious traffic may not be carried out thoroughly and actions to take in case of an incident occurring need to be put in place in line with security management principles. The risk of vast numbers of unpatched wearable devices, m2m systems, home automation and embedded appliances connecting to the Internet has been known to security experts for some time. Consequently, the first bot net of IoT devices was identified in 2013[8]. According to their data over a quarter botnetsare formed by devices other than computers, such as electrical appliances, smart TVs ,censors and other household utilities.

The economic benefits and new commercial opportunities presented by the IoT are evident and while the industry is still nascent, the investment into creating IoT –based revenue opportunities only in the U.S. have reached7.4 billion in 2014 [7]. However, as with many emerging technologies, addressing information security concerns of individuals remains secondary to business opportunities exploitation. Furthermore, privacy within the IoT realm remains within the reach of organisations exploiting the technology. Individuals are left with the same ‘digital-divide’ concern, and ‘if you are not in – you are out’ approach is adopted far too readily by smart device and technology manufacturer. The wearables are one of many examples tied deeply into the IoT consumerisation.

The tag of a healthy lifestyle has been attached to the wearable fitness devices, such as Fitbit ™. Tied to the information harvesting services of many insurance policies, individuals are left with little choice but to have every step tracked by third parties. Control over personal information in the IoT ecosystem is gradually taken away from the individual and its usage by third parties becomes ever less transparent to end users. The IoT surveys conducted in 2014 and 2015 by ISACA have shown that nearly half of IT professionals are concerned about IoT security and a quarter finds privacy unaddressed in the IoT developments. The problem of bring your own device (BYOD) into the organisational parameter has been taken to another level with the IoT threatening to shape BYOD policies into bring-your-own-ANYTHING. Any device may potentially be a part of the IoT, plugging into the enterprise network, while at present 60% of enterprises report their BYOD policy inadequate for wearables and nearly a quarter admit to not having a BYOD policy in place[7].

6 Directions For Future Research

The academic attention is drawn to three dimensions needing further research effort:

- Device and connectivity security: Devices with "always on" network connectivity are enabling new types of attacks and vulnerabilities of largely unsecured end point devices open new targets for potential data exposure and cybercrime perpetration.
- Identity, device and data management: Given the complexity of mobile device management, the challenges of IoT expand to management of billions of devices. It is important to highlight that the expectation of securing the enterprise IoT is reported to rest with the organisation (ISACA, 2015).
- Personal privacy in the IoT: a staggering majority (94% of users) are concerned or very concerned about the privacy being inadequately addressed in the IoT realm and are worried about the decreasing levels of privacy.

Existing conceptualisation of privacy is not considered sufficient in the IoT settings. The widely accepted three tier personal information privacy model proposed just under five years ago by [10] addressed the three tiers in personal information distribution paradigm. The personal information model comprised of three tiers:

1) Individuals, information about them was actively generated and deposited into the Internet domain
2) Service providers and vendors, were harvesting, processing and managing individual information from tier 1 and then generously distributed it onto third parties
3) Third parties, who commercialised personal information and exploited revenue opportunities from its use. These third parties were divided into malicious and benign according to their intentions and legal posture.

The control over personal information was firmly embedded within tier one and tier two. Extant researchers warn of the loss of control over personal information [9]. With the emergence of the IoT, the boundaries in the personal information control are eroded at the individual level and the personal information model no longer explains the information control layers within the interconnected ecosystem, where sensor and tracking devices are easily hacked. According to expert report it takes 10 seconds to run code injection on a Fitbit device, which later plugs into home networks and personal computing devices and distributes malware [5].

We would like to draw the research attention to the lack of individual skills to protect information privacy[2,9] and the blurring notion of individual information privacy rapidly dissolving in the overwhelming wave of sensing, tracking, reporting and transmitting devices individuals are connected to. The centre of any technology innovation are individual users, their views on information privacy should not be neglected by the commercial interests of IoT exploitation.

7 Conclusion

In this 'sense-making paper' challenges arising from the IoT ecosystem to the conceptualisation of individual privacy have been raised. The tangible benefits of the billions of interconnected devices are known to society and organisations. The dangers to personal information privacy within IoT must be addressed by vendors, manufacturers and service providers for the commercial opportunities of the emerging technology to be realised.

References

[1]. Bélanger, F., &Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. MIS Quarterly, 35(4), 1017-1042.

[2]. Benson, V., Morgan, S.&Filippaios, F. (2014). Social career management: Social media and employability skills gap. Computers in Human Behavior 30, 519-525.

[3]. Benson, V. Saridakis, G. &Tennakoon, H. (2015) Information disclosure of social media users: does control over personal information, user awareness and security notices matter?Information Technology & People28(3), 426 – 441.

[4]. EMC2(2014) The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things. Accessed on: 15/11/2015, available at :http://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm

[5]. Forbes Tech (2015) Fitbit Disputes Claim Fitbit Trackers Can Be Hacked And Infect PCs. Accessible at :http://www.forbes.com/sites/bradmoon/2015/10/21/fitbit-trackers-can-be-hacked-infect-pcs/ Accessed on 21/11/2015.

[6]. IDC (2014) Worldwide and Regional Internet of Things (IoT) 2014–2020 Forecast: A Virtuous Circle of Proven Value and Demand. Available at: https://www.idc.com/getdoc.jsp?containerId=248451. Accessed on: 21/11/2015

[7]. ISACA (2015) Isaca 2015 It Risk / Reward Barometer Report. Available at : http://www.isaca.org/SiteCollectionImages/Risk-Reward/2014/2014-Infographic-Global.jpg Accessed on 21/11/2015.

[8]. Proofpoint (2014) Proofpoint Uncovers Internet of Things (IoT) Cyberattack. Available at: http://investors.proofpoint.com/releasedetail.cfm?releaseid=819799. Accessed on 21/11/2015.

[9]. Saridakis,G., Benson,V., Ezingeard, JN and Tennakoon, H. (2015). Individual information security, user behaviour and cyber victimisation: an empirical study of social networking users. Technological Forecasting and Social Change

[10]. Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. MIS Quarterly, 35(4), 989-1016.

[11]. McKelveyB., Tanriverdi, H., &Yoo, Y. (2015) Complexity and Information Systems Research in the Emerging Digital World. MIS Quarterly. Available at: http://www.misq.org/skin/frontend/default/misq/pdf/CurrentCalls/MISQ_CALL_EmergingDigitalWorld.pdf