Transforming Healthcare with the Internet of Things
J. Hofdijk et al. (Eds.)

doi:10.3233/978-1-61499-633-0-31

Risk and the Internet of Things: Damocles, Pythia, or Pandora?

Chris SHOWELL[a,1]
[a] *eHealth Services Research Group, University of Tasmania, Australia*

Abstract. The Internet of Things holds great promise for healthcare, but also embodies a number of risks. This analysis suggests that the risks are as yet poorly delineated (having features in common with the oracle Pythia, and with Pandora and her box), and that adopting the precautionary principle is appropriate.

Keywords. Risk; Privacy; Computer Security; Internet

Introduction

The Internet of Things (IoT), is " an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and virtual world and react."[1] Smith and Erickson envision an IoT connected future in which "...the myriad embedded devices magically enhance our living environments, adjusting lights, temperature, music, medication, fuel flow, traffic lights, and elevators."[2]

For healthcare, the IoT represents an emerging sociotechnical environment which will change the way in which information and communication technology (ICT) is used, and is likely to provide a range of functions, including diagnosis, monitoring, treatment, and ambient assisted living. However, with any tantalising promise comes a range of poorly delineated or unknown risks. The IoT is a rapidly evolving ecosystem rather than a purpose designed healthcare environment. As Smith and Erickson note "…the IoT will probably grow organically, a global mashup of heterogeneous components with no top-down set of principles determining its emergent behaviour."[2] Each patient is likely to have an unpredictable, and uncurated collection IoT devices, including direct-to-consumer items, 'professional' devices recommended or provided by healthcare providers, and mundane domestic items. Because the management of this environment will be complex, it is appropriate to consider the threats and risks associated with these developments as examples of the *systemic* risks normally associated with threats to the environment. A framework for the analysis of systemic risk developed by the German Advisory Council on Global Change (WBGU) considers risk and damage, as well as the impact of uncertainty, ubiquity, persistency, reversibility, delay effects, violation of equity, and the potential for individual and community mobilisation.[3] This paper seeks to provide a broad, discursive overview of some of the challenges, which the IoT presents from the perspective of systemic risk.

[1] Corresponding Author.

1. Methods

The pace of development in the IoT is rapid and accelerating. Technical and financial barriers to the entry of new devices are low, and health-focused IoT devices and systems reside in an environment already crowded with such mundane items as refrigerators, toasters, and light globes. Taken together, these factors mean that risk likelihood and damage extent are not easy to estimate

In consequence a loosely structured approach has been taken to review security and privacy considerations, threats and risks, find examples of IoT incidents, and consider types of corporate behaviour which could have an effect on the use of the IoT for healthcare. A search in PubMed using the term “Internet of Things” returned 170 items. On review, all but 13 were discarded as not relevant, and only two described IoT risks. A comparable search in Google Scholar provided another three publications. The small number of retrieved publications may be a reflection of the rapid advance of the field. Searches in Google and Yahoo! for “Internet of Things” and “risk” or “fraud” yielded another 62 items (including blogs, and magazine and newspaper articles). These were reviewed to identify reported remote attacks, including on IoT devices, as well as likely avenues for future interference with IoT-based health-related processes.

2. Results

2.1. Security

Several challenges to health IoT were identified. Kozlov et al [4] detail a number of risks, including the user losing control of the device, interception of sensor data during transfer to a health provider, the unavoidable trade-off between usability and security, a potential misuse of personal identifiers following eavesdropping, theft of data from a data aggregation system, and targeted denial of service attacks. Identity theft, by impersonating the device’s IP address (IP spoofing) or MAC address (ARP spoofing) was also reported as a risk.[5] Reback and Costello [6] warn that “IoT development could increase security vulnerabilities at both the individual and systemic levels. Part of the problem is that while a variety of new "things" are being connected to the Internet, the manufacturers of these objects may not have either the experience or expertise to implement appropriate security safeguards.”

2.2. Privacy

Ensuring the privacy of health data is a matter of concern for a significant proportion of patients. Papoutsi et al [7] found that 79% patients had concerns about the security of their data within an electronic health record. Typically, the privacy protection offered to end-users of commodity technology is provided on the basis of ‘notice and consent’ – users are asked to read extensive details about how their data will be used, and then consent to the terms that are offered. Since many IoT devices lack a user interface, it is not clear how the privacy conditions will be agreed to.

Baby monitors also present a threat to privacy. Weaknesses in the camera software have allowed hackers to remotely access a number of Internet-connected baby monitors, and communicate verbally with the monitored infants.[8]

"By connecting to Wi-Fi, these so-called Internet of Things (IoT) devices allow access from wherever the owner is in the world, but…these devices are often so poorly secured, it takes little effort for a hacker to gain access." [9]

2.3. Maintenance and update

Most software driven devices require periodic updates to ensure that they continue to operate appropriately, and are protected against vulnerabilities. IT professionals may find it challenging to determine whether a computer is affected by a newly identified vulnerability; updating IoT device operating systems and applications will be onerous for consumers with sound technical skills, and near impossible for those without. "Left unperturbed, the commercial/industrial IoT sector might prove to be the Windows XP of the IoT, full of homogeneous badness that won't go away and persisting through an unwillingness to embrace improved, potentially safer systems."[2]

2.4. Hacking examples

There are already several examples of hacking attacks affecting IoT devices, as well as larger Internet-connected healthcare appliances. Two security researchers remotely accessed nearly 70,000 medical systems within a large US healthcare organisation, including "…21 anaesthesia, 488 cardiology, 67 nuclear medical, and 133 infusion systems, [and] 31 pacemakers".[10] In 2015 the US Food and Drug Administration issued a warning that a model of infusion pump in common use in hospitals was vulnerable to cyber attack, and recommended withdrawing the pumps from use.[11]

When Dick Cheney's defibrillator was replaced in 2007, the wireless interface was inactivated to minimise the risk of assassination.[12] In July 2015 Charlie Miller and Chris Valasek demonstrated their ability to control the radio, climate control and accelerator of a Jeep Cherokee by remotely accessing the car's control systems.[13]

2.5. Corporate behaviour

There have been several reports of actions and strategies of dubious ethical standing which are seen as 'business as usual' for large corporations.

Corporations may knowingly lie about or obscure the function of a device. Volkswagen manipulated the software in its Jetta diesel engines to disable the emission control system except when a vehicle appeared to be undergoing laboratory emissions testing. [14] Samsung issued a statement denying that the power saving "motion lighting" feature in their televisions had been specifically designed to give misleading results in IEC power consumption tests, although that was an effect of the feature.[15] The everyday operation of late model John Deere tractors is managed by proprietary software that the manufacturer has protected by copyright, effectively preventing maintenance by any but company-licensed mechanics.[16] Inspection of the software to confirm its method of controlling the tractors' functioning is technically illegal.

Corporations may seek to manipulate health evidence or consumer behaviour. Coca Cola has been criticised for providing financial and logistical support to the Global Energy Balance Network, a research organisation that promotes the idea that a lack of exercise, rather than the consumption of a sugar-rich diet, is the primary cause of obesity.[17] Health insurers are looking to use IoT monitoring of clients to better manage risk and reduce payments.[18] Amazon's WiFi connected 'Dash' device facilitates the reordering of household products from Amazon at the push of a button, and when added to washing machines, the functionality allows the automatic ordering of washing powder when more is needed. The user does not see the cost of the transaction in either case.[19]

3. Discussion

There are several criteria by which the success of the IoT in healthcare might be evaluated. Ideally, any use of the IoT should: support the provision of effective, high quality, evidence-based care; protect patient safety; ensure patient privacy; secure data from loss during communication; and be free from commercial bias or distortion. However, each patient home could already have IoT devices such as light globes, refrigerators and doorbells, with different vendors, standards, and security and privacy settings. One insecure or poorly configured device within a home IoT network could provide access to most (or all) other devices on the network. There is almost certainly no competent technical professional curating or supporting this collection, making it challenging to meet the criteria outlined above.

Using the Internet of Things in the provision of healthcare will inevitably reproduce some existing risks associated with the use of ICT, such as threats to security and privacy, and the loss or delay of data in transit. However, the exponential increase of endpoint devices and intermediate equipment magnifies the number of items at risk, and places many devices in a poorly controlled environment, leading to changes in the likelihood of those risks. Use of the IoT also introduces new risks to patients from the exposure to commercial decisions without a mandated guarantee of ethical behaviour.

The German Advisory Council on Global Change (WBGU) has associated six clusters of systemic risk with characters from Greek mythology – Damocles, Cyclops, Pythia, Pandora, Cassandra and Medusa – the underlying narrative for each character matches the nature of the risk.[20] Damocles was invited to be ‘king for a day’. On taking the throne, he found above him a sword hanging by a slender thread; ‘Damocles’ type risks have a high probability of damage, but a low likelihood. Pythia, a noted Delphic oracle, gave prophecies, which were highly valued, but ambiguous and hard to interpret; both the probability of ‘Pythia’ risks and the extent of damage are uncertain. When Pandora married, the gods gave her a closed box containing many evils, and told her to keep the lid closed. She opened it, releasing those evils upon the world. ‘Pandora’ risks involve extensive changes with no clear link to resulting damage; adverse effects emerge only after extensive spread of the changes has occurred.

The evolving risks associated with the IoT are unlikely to be risks of Damocles. They are more likely to have the nature of Pythia – neither the evidence of risk nor the extent of the damage will be immediately apparent. Over time, those risks will exert their effect, and in retrospect an absence of prior caution will become apparent. Risks characterized by Pandora may also eventuate. The changes brought by the IoT for healthcare will result in damage in the future, but the connection between the risk and the damage will not be immediately obvious. Once the link is made, it will be too late to reverse the changes. Renn and Klinke [21] identify the precautionary principle as the appropriate strategy for managing both types of risk.

What does the precautionary principle entail for a health IoT? As an ideal, new implementation should be supported by sound evidence of patient outcomes, safety, and benefits, with those benefits outweighing the costs of implementation, use and maintenance. There should also be a well-defined framework for the long-term management of IoT devices, including the issuing and revoking of trust certificates, updating software, and eventual device retirement. One way of ensuring these ideals are met would be through control and regulation, although it seems that the time for such an approach may have passed, with no regulations in place. While most providers of health ICTs are ethical, focus on the needs of patients, and would comply with regulation, we should expect there would be a handful of individuals and firms who do not. Regrettably, this brief overview highlighting some of the likely risks inherent in health IoT cannot provide a clear way forward, but should serve as a warning that the precautionary principle must be applied.

References

[1] ISO/IEC JTC 1. Internet of Things (IoT) Preliminary Report 2014. 2014.

[2] Smith SW, Erickson JS. Never Mind Pearl Harbor–What about a Cyber Love Canal? IEEE Secur. Priv. 2015 Mar;13(2):94–8.

[3] OECD, editor. Emerging systemic risks in the 21st century: an agenda for action. Paris: OECD; 2003.

[4] Kozlov D, Veijalainen J, Ali Y. Security and Privacy Threats in IoT Architectures. ACM; 2012 [cited 2015 Oct 6]. Available from: http://eudl.eu/doi/10.4108/icst.bodynets.2012.250550

[5] Vidalis S, Angelopoulou O. Assessing identity theft in the Internet of Things. IT Converg. Pract. 2014;2(1).

[6] Reback S, Costello T. Deconstructing the Internet of Things. Bloom. Gov. [Internet]. 2014 [cited 2015 Oct 6]; Available from: http://www.webcitation.org/6dvhzdKPn

[7] Papoutsi C, Reed JE, Marston C, Lewis R, Majeed A, Bell D. Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: results from a mixed methods study. BMC Med. Inform. Decis. Mak. [Internet]. 2015 Dec [cited 2015 Oct 23];15(1). Available from: http://www.biomedcentral.com/1472-6947/15/86

[8] Hill K. The Half-Baked Security Of Our “Internet Of Things” [Internet]. Forbes. 2014 [cited 2015 Oct 22]. Available from: http://www.webcitation.org/6dviHRyxN

[9] Whittaker Z. New security flaws found in popular IoT baby monitors [Internet]. ZDNet. 2015 [cited 2015 Oct 22]. Available from: http://www.webcitation.org/6dviMrwO4

[10] Pauli D. Thousands of “directly hackable” hospital devices exposed online [Internet]. The Register. 2015 [cited 2015 Oct 22]. Available from: http://www.webcitation.org/6cTqrpe1w

[11] Center for Devices and Radiological Health. Safety Communications - Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication. 2015.

[12] Gupta S. Dick Cheney’s heart [Internet]. CBS News. 2013 [cited 2015 Oct 22]. Available from: http://www.cbsnews.com/news/dick-cheneys-heart/

[13] Miller ME. How hackers can control your car from miles away [Internet]. Wash. Post. 2015 [cited 2015 Oct 22]. Available from: http://www.webcitation.org/6dviRi3xR

[14] Topham G, Clarke S, Levett C, Scruton P, Fidler M. The Volkswagen emissions scandal explained. The Guardian [Internet]. 2015 Sep 24 [cited 2015 Oct 23]; Available from: http://www.webcitation.org/6dviXUjcl

[15] Neslen A. Samsung TVs appear less energy efficient in real life than in tests | Environment | The Guardian [Internet]. 2015 [cited 2015 Oct 5]. Available from: http://www.webcitation.org/6dvibkrx2

[16] Sydell L. DIY Tractor Repair Runs Afoul Of Copyright Law [Internet]. NPR.org. 2015 [cited 2015 Oct 23]. Available from: http://www.webcitation.org/6dvifO3qx

[17] O’Connor A. Coca-Cola Funds Scientists Who Shift Blame for Obesity Away From Bad Diets [Internet]. Well - NYT. 2015 [cited 2015 Oct 23]. Available from: http://www.webcitation.org/6dvik99SZ

[18] Borst M. Insurance In The Age Of The Internet Of Things [Internet]. Digit. Mag. 2015 [cited 2015 Oct 5]. Available from: http://www.digitalistmag.com/industries/insurance-age-internet-things-02361459

[19] Fleishman G. Don’t dash to Dash: new Amazon buttons aid brands, not consumers [Internet]. TechHive. 2015 [cited 2015 Oct 23]. Available from: http://www.webcitation.org/6dvipDXFB

[20] German Advisory Council on Global Change (WBGU), editor. World in transition: strategies for managing global environmental risks. Berlin: Springer; 2000.

[21] Renn O, Klinke A. Systemic risks: a new challenge for risk management. EMBO Rep. 2004;5(1S):S41–6.