# UBIQUITY, SECURITY AND YOU – MALWARE, SECURITY AND THE INTERNET OF THINGS

*Jasmine Sesso*
Microsoft, Australia

*Heather Goudey*
Independent researcher, Australia

Email jasmine.sesso@microsoft.com; heatherg@roninwriters.com

## ABSTRACT

The Internet of Things (IoT), is an omnipresent and complex system of systems, where the billions of objects that make up our physical environment are identified, labelled, virtualized and connected. Massive amounts of data are gathered from a multitude of omnipresent sensor nodes, and analysed to solve difficult, real-world problems. The applications of these systems are seemingly endless and range from automating your whole house, to monitoring your health and managing large-scale industry. The future proposed by this recent computing paradigm is exciting, and some of it is already here today.

However, even a brief analysis of the possible implications of this type of ubiquitous computing suggests a more dystopian outcome. While the wonders of the IoT are many and varied, the privacy and security implications are somewhat unknown. By 2020, it is estimated that there will be approximately 50 billion nodes in operation worldwide. Even if you choose not to be virtualized by the IoT, escaping unrecorded by its many nodes will be nigh on impossible, and its tangible effects on physical systems mean that traditional notions of what constitutes risk will need to be rethought. One thing is certain though: the threats of malware have never been more real.

The next logical step in the evolution of the Internet – the IoT – promises many things, including futuristic smart cities, more efficient use of dwindling resources and advances in almost every industry and area you care to mention. From the cybernetics in your body, to the car that you drive, to the food on your plate, the IoT makes 'ubiquitous computing' our new reality. Even ignoring the hype (of which there is much), have no doubt that we are looking at a new computing paradigm with potentially profound effects on how we work, how we interact with the world around us, and how we live. However, regardless of the concerted efforts of many working groups and consortiums, the IoT continues to pose some particularly difficult problems for security – problems that could severely limit its acceptance and true potential.

This paper looks at the state of the AV industry in the context of the IoT in 2015, then drills down into the specific security implications faced, as well as, the current approaches taken to address them. We examine the behaviour of current malware already found in the wild targeting the IoT, extrapolate trends, take a critical look at recent recommendations from the FTC's (Federal Trade Commission's) 'Internet of Things – Privacy and Security in a Connected World' staff report, and discuss the relevance of AV in this brave new world.

## UTOPIA OR DYSTOPIA?

The IoT can be glimpsed on the horizon. Current thinking is that we are approximately five to ten years away from its wide-scale adoption ([1], p.113) and the estimated number of objects that will be connected by 2020 keeps rising (the figure varying considerably depending on the source – from 20 billion to 200 billion [2–5]). While the concepts of ubiquitous and ambient computing have been around for some time, and the phrase 'Internet of Things' was first coined over 15 years ago [6], interest in the IoT has recently reached a critical point.

With possible applications ranging from manufacturing to healthcare and managing entire cities (with everything in between), and a convergence of affordable enabling technologies in computing, sensing, networking and storage, not to mention IPv6, the sky's the limit. The economic impact for the industries involved is also particularly significant (let alone the functional and conceptual impacts for humanity). Returning to the magical 2020 date, *Gartner* predicts that 'product and service suppliers will generate incremental revenue exceeding $300 billion' by this time [2]. It is expected to be a considerable driver of economic activity and development ([7], p.2787). Unsurprisingly, some of the biggest names in the IoT are the biggest names in other 'things' as well – notably those involved in the tangible results of the convergence of computing, networking and communications. They include *Axeda*, *AT& T*, *Cisco*, *Google*, *IBM*, *Intel*, *Microsoft*, *Qualcomm*, *Samsung*, *Salesforce.com*, *Sprint* and *Verizon* amongst a growing number of others.

So, here we stand on the edge of the IoT – an Internet, but better because the information it captures, contains and consumes is created and managed by 'things' (machines) unfettered by the highly fallible intrusion of human-generated data. Thus, with 'computers that [know] everything there [is] to know about things – using data they gathered without any help from us – we [can] track and count everything, and greatly reduce waste, loss and cost' [6]. This is the utopian promise of IoT – with accurate, detailed, wide-ranging data captured from the physical world, we can make huge gains in efficiency and reduce the wastage of increasingly scarce resources. Yet, it's the capture, transmission and storage of that data that fuels the dystopian visions of IoT as well – where privacy is all but lost and powerful forces influence and act on us in illegitimate, unwanted, or even possibly malicious ways. With the virtualization of the objects that comprise reality, the stakes of compromise or ill-use are higher too – it's bad enough when attackers compromise your electronic bank account, imagine if they could hack your house as well! The implication is that, regardless of how smart the device or range of devices is, if you connect it, you can hack it. Unfortunately, it's just as easy to imagine terrifying outcomes for this technology, as it is wondrous advances in human ingenuity.

## THE ELEPHANT IN THE ROOM

At a functional level, the IoT is an omnipresent mix of billions of IP-connected embedded objects, smart devices, sensors and actuators with web services in between ([1], p.113). Many sensors are already in use in different areas as they are cheap to produce and easy to deploy and use the existing Internet for access ([7], p.49). The key features here are complexity and heterogeneity, but note also that objects in the IoT are often widely distributed and highly constrained with regard to energy, memory and processing. In the IoT, objects only need

enough resources and functionality to complete their very particular objectives (for example, data collection, transmission, or processing). Conceptually, objects in the IoT share a number of particular characteristics, including existence, self-awareness, interactivity, context awareness and dynamicity ([8], p.52). The security challenges of the IoT arise specifically out of these functional and conceptual characteristics. Ning *et al.* group these obstacles to confidentiality, integrity, and availability into three main areas – scope, dynamicity and heterogeneity ([10], p.46).

The potential scope of the IoT is mind-boggling. As mentioned above, the closer we get to adoption, and the more applications we envisage for the technology, the more the projected numbers of objects rise. This scope is beyond anything we have seen or had to deal with before – it is certainly beyond the capacity of mere humans to manage, and the use of automation will be necessary. It also has the potential for multiple points of failure and necessitates significant redundancy, fault awareness and tolerance. It is not inconceivable for proposed solutions to need to scale to at least billions of objects ([9], p.53) and for many of those objects to be vastly unattended and prone to physical interference or malicious attack ([1], p.113). And of course, it's not just the number of objects but the amount of data that will be collected and transmitted. The more data is captured, the more accurate the control decisions made and the smarter the smart devices with which we interact directly ([11], p.34). However, the more data that is gathered, stored and transmitted, and the more abstraction that is required in order to make the data meaningful for control decisions, the greater the importance of ensuring confidentiality, integrity and availability of that data – and yet the harder that is to accomplish.

The required dynamicity of the IoT brings issues as well and is a significant challenge to some of our current concepts of ICT security. Objects in the IoT need to be able to interact with many different things at different times. The beauty of the proposed IoT comes with its ability to gather data and react in real time to changing conditions. This may also require an object to both 'create and consume a large number of services' ([9], p.52). When we think of secure communications on the Internet today, we often think of secure end-points with secure point-to-point communications in between ([12], p.2) – so trust exists while a secure client has a secure connection to a secure server but is gone when that connection is over. But the IoT is not a connection-oriented system, and as many current security protocols are connection-oriented, this brings into question their applicability in this area. Even though there are arguments for continuing to use a centralized cloud-centric approach for IoT, making management, data processing and physical security easier ([11], p. 32), a more peer-to-peer approach is more in line with the IoT conceptually. In the IoT, problems and processing are distributed, with many nodes operating as servers in some instances, as clients in others, depending on context and changing conditions. (We should also note at this point that some of the solutions currently being discussed for IoT security, such as lightweight implementations of IPSec and DTLS are connection-oriented).

The third major obstacle is posed by the heterogeneity in the systems that comprise the IoT. While there have been some efforts with regard to implementing standards (such as work done by the groups of companies in the Open Interconnect Consortium [13] and the Industrial Internet Consortium [14]) the IoT essentially consists of lots of different technologies cobbled together in ways that were not necessarily intended and that may introduce gaps that produce data leakage or worse. The rush to market and the pressure to keep costs down is seeing different technologies repurposed and being used together in unexpected ways, and without working standards, the connections between them are less than seamless. Transparency is also an issue (although not one that is limited to the IoT) and much technology may be built on older insecure technology. Actually determining what's in the stack and what vulnerabilities are in play is not necessarily an easy question to answer, but examples like Heartbleed make answering that question a priority. Of course, even if you can determine exactly what technology is in use and what it may be vulnerable to, that doesn't mean that patching is viable or even possible – the highly constrained nature of the objects in the IoT means that some components will remain vulnerable indefinitely – and that traditional solutions to security problems may not be viable or even possible.

While we can see that there are considerable security issues posed by the IoT with regard to its current characteristics of massive scope, dynamicity and heterogeneity, it is also worth making a particular note of the challenges it poses to privacy. The amount of data being gathered will be on a scale hitherto unseen, but it's really the *types* of data potentially being gathered that pose a bigger concern. Even if you don't want to be part of the IoT, without a type of personal cloaking device, how could you possibly escape from having your personal information monitored, recorded and stored when the sensors are omnipresent in your environment? Data that we think of as benign can take on a different meaning in aggregate. Addressing privacy concerns is going to require a particularly special effort, and users will need tools, information, and support to understand what's at stake, to know who has their data and how it is being used, and to be able to manage their own data and determine access to their data as they see fit ([9], p.54).

So, as we can see, the IoT is potentially amazing – more than a game changer, but its conceptual and functional characteristics pose very significant security problems with risks to privacy being particularly concerning. There are challenges at every level to confidentiality, integrity and availability, and additional issues with regard to authentication, authorization, anonymity, trust and non-repudiation (the issues run like a security 101 checklist), and they leave these systems vulnerable to compromise. Possible attacks against IoT systems range from skimming or eavesdropping to possible spoofing, replaying, or denial of service (and every shade in between) ([10], p.47). The stakes are high as the consequences of attacks have tangible, even visceral outcomes. Addressing these challenges requires work in multiple areas on multiple levels, and the problems that must be solved include finding suitable cryptographic and network mechanisms, the means to manage the vast hoards of data appropriately, and trusted architectures that still satisfy the functional requirements of the potential IoT, outside the box of our server-client, centralized cloud-centric blinkered thinking. Of course, none of these concerns are new – they are known knowns – and many groups are working towards addressing these concerns in conceptual and practical ways.

## CURRENT APPROACHES TO SECURING THE IOT

The Industrial Internet Consortium and the Open Interconnect Consortium are working towards standards that will support interoperability while taking security into account at the same time. There are also a number of existing standards that might address particular aspects of IoT security (including IEEE P1363, IEEE P1619, IEEE P2600, IEEE 802.1AE and IEEE 802.1X) ([15], p.53). Research is ongoing into many different approaches to the problem from different angles, including in the areas of cryptographic mechanisms, embedded security, secure applications, and novel frameworks ([1], p.113). Progress is even being made, with the IETF deciding to use DTLS (Datagram Transport Layer Security) to secure communication between constrained devices using CoAP (Constrained Application Protocol), but questions remain regarding its applicability, with concerns that it doesn't scale and that it continues to use a connection-oriented model that doesn't work particularly well for the full-scale, ubiquitous IoT as envisaged ([12], p.2).

The current research might not have all the answers, but it does recognize the importance of particular characteristics of the solutions required. Due to the functions of the IoT and its related constraints, solutions need to be:

- Lightweight
- Largely automated
- Able to provide assurance for the confidentiality and integrity of data
- Self-aware and context-aware (for example, able to recognize the state of the systems it interacts with)
- 'Things-centric' (as opposed to 'Internet-centric')
- Considerate of privacy
- Scalable (yet fine-grained enough to deal with heterogeneity)
- Able to adapt to changing data streams and future uses
- Robust
- Fail safe
- Dynamic.

This is a long list of requirements, but if we're serious about making 'security by design' more than a marketing buzzword then this is exactly what's required. At this particular point in time, considering the problems posed by the nature of the technology that makes up the IoT, pragmatic solutions are more likely to recognize the limitations of traditional notions of security in this context. As such, a combination of network and object monitoring that reports changing and aberrant states relative to what is normal for that environment is a possible solution. Used with limited rule-sets and whitelisting for constrained devices, a bump-in-the-wire approach for network monitoring, and use of the cloud for more intensive processing and analysis of behaviours might provide some notion of security.

As history has demonstrated, one of the biggest deal breakers with the public is a lack of security and trust. However, when it comes to the uptake of new technology, it's often more about economics – users need to be able to trust the systems they interact with in order to take the plunge and spend the money. The same arguments we heard about going online to do our banking and our shopping are being touted again for IoT – if you can't secure it, will they come? While there is no doubt that many different groups are thinking of security and actively working on the problems at hand, several experts seem to be in agreement about the nature of security on the IoT, and again it's a matter of economics: many components of the IoT are highly constrained and cheap, which makes security mechanisms hard and expensive. Marketers are too concerned with getting their product to market to consider security, and technology is rapidly being repurposed ([15], p.53). The real impetus for security is likely to come from an economic driver as well – they'll build it, people will come, crime will move in (according to opportunity crime theory), something will go wrong, then security will be front and centre, and the costs will be worthwhile because of the significant risk posed by what's going on in the wild. With that in mind, we turn next to look at the current evidence being reported from the wild.

## SNAPSHOT FROM THE WILD AND WHAT TO EXPECT NEXT

While current evidence suggests that perhaps the IT industry is already behind in security efforts [16], collectively we ought not to be defeatist; investing in securing the device, user education and prevention should be part of our plan moving forward.

At the time of writing this paper, we are not aware of any current threats *affecting* IoT devices. However, numerous proofs of concept (POCs) exist. It is worth noting that just because no active *attacks* have been disclosed, it does not mean that attacks aren't occurring; rather, they may not yet have been detected or disclosed.

Currently, there are few big names in the AV industry[1] marketing real-time protection for IoT devices. Presumably a vast number of these devices do not receive ongoing support or monitoring for security breaches from the developer (nor will computationally-intensive, traditional approaches to perimeter-based security work in this context); thus, opportunities to effectively monitor to detect malware or other security breaches might be somewhat limited. (One way protection could be improved is by embedding technology by which nodes have the ability to report their state, or at least recognize bad states, which will be discussed later).

However, we have seen home security camera systems and baby monitoring devices being hacked by exploiting default security passwords and unsecured networks, and POCs of IoT-connected health devices being hacked [17–22]. Often, the root of these exploits and compromises are poor security practices; nothing more, nothing less.

Recent chilling press coverage might have you believe that a refrigerator fell victim to an attack and was used as a spambot to distribute thousands of spam emails; however, further investigation showed that, while the fridgebot appeared to be the source of this evil, in fact it was an infected PC that shared a router with the connected refrigerator that was to blame [23–25]. 'So what if my refrigerator is infected?', you might ask. While this might seem like a relatively innocuous attack scenario, the implications of having your refrigerator

[1] Note, however, that *McAfee* is working as part of *Intel* on security for medical devices: http://newsroom.mcafee.com/press-release/security-essential-iot-and-networked-medical-devices.

or any other appliance in your home infected by malware is significant. Consider all the data that could be collated about you and your co-inhabitants, should a handful of your devices be compromised. Just for starters, your refrigerator can tell attackers when you're home, what you're consuming, when you're shopping, and possibly where you're shopping. Needless to say, businesses are also at risk. A business could use connected refrigerators and cool-rooms to monitor and control the temperature changes of a number of units, setting up alerts if and when temperatures fall into danger zones to help reduce the risk of food spoiling. If an attacker were to gain control of the monitoring system and disable alerts or adjust the temperature in order to spoil the food, deliberately sabotaging the business, the consequences could be very costly. Consider also the same scenario in a temperature-controlled lab containing millions of dollars' worth of pharmaceuticals.

If history were to repeat itself, we might start to see some relatively innocuous threats targeting IoT devices, before more nefarious threats begin to emerge. For instance, might we see devices being turned off and on at the attackers' command, car doors being locked and unlocked, temperatures and timers on heating and cooling devices being re-set at random? What's to say this might not soon be followed by whole-home surveillance and data-gathering, and widespread exploiting of personal fitness and healthcare information?

## FTC RECOMMENDATIONS AND CRITIQUE

In a comprehensive report by the Federal Trade Commission (FTC), the authors detail their recommendations for Congress to develop general data security legislation, as opposed to IoT-specific legislation [26]. We believe this is a good starting place, but are not convinced these recommendations go far enough.

While the FTC report acknowledges that the privacy and security risks to IoT-connected devices are very real, it states that any IoT-specific legislation risks stifling innovation. We don't disagree with these recommendations ([26], p.48), but they are very general in nature, and do not make a real call to action. Legislation for businesses and developers, even if general in nature, will help build awareness on user privacy and security risks, but is unlikely to deter hackers or prevent attacks.

Currently, one of the most 'successful' attack vectors in the wild is exploiting vulnerabilities. Given the 'success' attackers have exploiting vulnerabilities, we can assume that this behaviour will transition to IoT devices, provided there is opportunity. If reports that 'six out of ten IoT devices suffer vulnerabilities', or worse still, *all* IoT devices are proven to be vulnerable, we need to act now to improve the foundations of the technology on which we are building these devices [27, 28].

We acknowledge the challenges that IoT device developers face regarding patching low-cost (or disposable) devices that often have low or no interface. However, here lies an area begging for innovation; how can we continue to educate and advise users, giving them the consent and control they need and want [29]? Can developers continue to support users and protect their devices from being exploited? This potential attack vector won't be addressed by legislation; we need to be more creative in our protection approach. What we need is to invest in systems and methods by which we detect a compromised device, recognize bad states, and manage the compromise. Fast and effective triage needs to occur to determine appropriate action. Fast, effective, and cheap. The response needs to be robust and automated – the potential here for machine learning is incredible.

The FTC also recommends 'self-regulatory programs' as a means to 'encourage the adoption of privacy- and security-sensitive practices' ([26], p.49). Again, while we support this initiative, we're not convinced it could ever prove a successful prevention technique; these authors have not been able to find an example of a successful self-regulatory program in technology.

The FTC discusses, at length, the importance of limiting the information devices collect, and the risks associated with data retention ([26], p.51). It recommends, in addition to revising privacy legislation, that developers carefully consider the amount of data collected and the means by which the data is stored, and that they take action to limit the amount of data collected and stored. Complementing this, the report recommends that developers proactively 'seek consumers' consent for collecting additional, unexpected categories of data'. We wholeheartedly support these calls to action, and see this as an area for great innovation, be this in the area of user education or ongoing user engagement.

## AV'S ROLE IN THE BRAVE NEW WORLD – THE PROBLEM AND THE OPPORTUNITY

Remember years ago when it seemed like we might actually have the malware problem licked? And remember when it got really bad again and malware numbers exploded? And then the industry got creative and applied big data, behavioural and dynamic cloud-based approaches and again we thought maybe we were getting somewhere? Now we're telling you that we're going to have to rethink this again with IoT, but of course we don't have to throw away what we already have. We know this. We're the experts here and there is an opportunity for the AV industry to be front and centre in this discussion because the knowledge and experience in this industry is key to addressing these issues.

There is a broad consensus in the industry that we need to secure the IoT and its devices [30, 31]. We know some AV companies are investing in embedded security technology to help protect devices [32–35]. As always, considerations around cost and performance are important, especially when the device scale is so broad; from tiny, inexpensive *Fitbits* to large, costly medical machinery. Room remains in this field for new, as well as existing players to step up and work together to secure IoT technology.

For one thing, we're pretty familiar with the rules-based approaches that will be necessary in highly constrained environments (even if signature-based detection may have long been our forte) and as an industry, our knowledge of threats and our long association with wide-scale commodity malware and APTs gives us unique insight into the expected projection of threats in the IoT. Threat modelling will be key to ensuring that protective mechanisms are specific and targeted enough to meet the lightweight requirements of protection going forward. Certainly, our traditional, heavy computational or centralized approaches might not work as well here, but our experience with the analysis of threats from

a big data perspective puts this industry in a unique position as a potential leader and trusted advisor to the many other businesses that will come.

## CONCLUSION

So, as we've seen, the security issues for the IoT are not insignificant. Many of the problems really do continue to fall into the 'too hard' basket and will be likely to remain there for some time. While there is no doubt that conversations around securing the IoT are continuing to gain momentum in industry, academia and the popular press, it is the push to get technology to market and to gain market share that is really calling the shots here. We expect that, as much as we talk about it, and as good as many security researchers' intentions are, security will be late to the IoT party. It will only be with the threat and experience of real compromise and loss that security implemented in practice will move beyond the stage of 'mostly reactive'.

But there is opportunity here – for the people in this audience in particular. There is an opportunity for developers to create innovative security solutions to the privacy problems that will no doubt arise. There is an opportunity for providers in this industry to lead conversations and apply their knowledge, experience, wisdom, and innovation to these problems. The potential for dystopian outcomes is not overstated, but of course, you need to ask yourself where's the value and what's the risk? Just because something is vulnerable, doesn't mean that it will be targeted. Like the devices we're so enamoured with, we're going to have to be smarter to address the issue of security in the IoT.

This paper has but touched on some of the issues involved, the concepts being applied to address them and current evidence from the wild. If anything, it points to more problems than it answers, and as authors, we acknowledge this. However, even taking its considerable limitations into account, the process of protecting users and organizations, at least conceptually, from threats via the IoT means engaging in the same activities that we're already familiar with – educating users, monitoring the environment for anomalous behaviour, knowing the threats, limiting privileges and functionality to the task at hand, knowing your technology stack, understanding the value of your assets, prioritizing security investments appropriate to potential impact and, perhaps above all, *expecting* to be compromised. The secret to successfully protecting the IoT might be realizing that it can't be protected – and then working out how we continue to operate in an environment that is inherently insecure and is highly likely to remain so, perhaps indefinitely. Yes, the security problems are great, and the risks are high, and we haven't really come to terms with what ubiquitous computing really means for us as a civilization, but we're very familiar with imperfect security. We live it every day.

As the experts here we ask you to respond to this call to action: be proactive in this discussion. Engage with the IoT industry and share your wisdom in the art of putting security first. Be generous with your knowledge and experience so we can help prevent bad security practice mistakes, know the threats, and avoid possible dystopia. And you never know – by ensuring that you're a part of these discussions and using your influence, it might even help your AV business.

## REFERENCES


[1] Ashraf, Q. M.; Habaebi, M. H. Autonomic schemes for threat mitigation in Internet of Things. 2015. Journal of Network and Computer Applications, vol.49, pp.112–127.

[2] Internet of Things will transform the data center. Gartner press release. 19 March 2014. http://www.gartner.com/newsroom/id/2684616.

[3] Press, G. Internet of Things by the numbers: Market estimates and forecasts. Forbes. 22 August 2014. http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/.

[4] Evans, D. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. 2011. https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[5] Zaslavsky, A. Internet of Things and Ubiquitous Sensing. Computing Now. 2013. http://www.computer.org/web/computingnow/archive/september2013.

[6] Ashton, K. That 'Internet of Things' thing. RFID Journal. 2009. http://www.rfidjournal.com/articles/view?4986.

[7] Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. 2010. Computer Networks, vol.54, no.15, pp.2787–2805.

[8] Skarmeta, A.; Moreno, M. V. Internet of Things: Security, privacy and trust considerations. 2014. Lecture Notes in Computer Science, pp.48–53.

[9] Roman, R.; Najera, P.; Lopez, J. Securing the Internet of Things. Computer, vol.9, no.9, pp.51–58.

[10] Ning, H.; Liu, H.; Yang, L. T. Cyberentity Security in the Internet of Things. Computer, vol.46, no.4, pp.46–53.

[11] Want, R.; Schilit, B. N.; Jenson, S. Enabling the Internet of Things Computer, vol.48, no.1, pp. 28–35.

[12] Vucinic, M.; Tourancheau, B.; Rousseau, F.; Duda, A.; Damon, L.; Guizzetti, R. OSCAR: Object Security Architecture for the Internet of Things. Ad Hoc Networks. 2014.

[13] Open Interconnect Consortium. http://openinterconnect.org/.

[14] Industrial Internet Consortium. http://www.iiconsortium.org/about-us.htm.

[15] Grau, A. Can you trust your fridge? 2015. IEEE, New York, pp.52–55.

[16] Grange, W. The Botnet of the Internet of Things. Blue Coat Labs. 2015. https://www.bluecoat.com/security-blog/2015-01-09/botnet-internet-things.

[17] Matyszczyk, C. Hacker shouts at baby through baby monitor. CNet. 29 April 2014. http://www.cnet.com/news/hacker-shouts-at-baby-through-baby-monitor/.

[18] Hill, K. 'Baby monitor hack' could happen to 40,000 other foscam users. Forbes. 27 August 2013.

http://www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/.

[19] Hill, K. How your security system could be hacked to spy on you. Forbes. 23 July 2014. http://www.forbes.com/sites/kashmirhill/2014/07/23/how-your-security-system-could-be-used-to-spy-on-you/.

[20] Smith, M. Peeping into 73,000 unsecured security cameras thanks to default passwords. Network World. 6 November 2014. http://www.networkworld.com/article/2844283/microsoft-subnet/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html.

[21] Robertson, J. Hacker shows off lethal attack by controlling wireless medical device. Bloomberg. 29 February 2012. http://go.bloomberg.com/tech-blog/2012-02-29-hacker-shows-off-lethal-attack-by-controlling-wireless-medical-device/.

[22] Tolentino, M. Pacemakers under attack: When the internet of things gets sick. Silicon Angle. 20 August 2013. http://siliconangle.com/blog/2013/08/20/pacemakers-under-attack-when-the-internet-of-things-gets-sick/.

[23] Bort, J. Refrigerator hacked: Here's the biggest problem facing the Internet of Things. January 2014. Business Insider. http://www.businessinsider.com.au/hackers-use-a-refridgerator-to-attack-businesses-2014-1.

[24] Bonner, S. Hacked by your fridge? When the Internet of Things bites back. 2014. The Guardian. http://www.theguardian.com/media-network/media-network-blog/2014/feb/28/internet-things-hacked-security.

[25] Storm, D. Blame infected Windows PCs, not smart fridge, for spam-spewing botnet attack. ComputerWorld. 27 January 2014. http://www.computerworld.com/article/2475725/cybercrime-hacking/blame-infected-windows-pcs--not-smart-fridge--for-spam-spewing-botnet-attack.html.

[26] Federal Trade Commission. Internet of Things: Privacy and Security in a Connected World. 2013. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[27] HP Study Finds Alarming Vulnerabilities with Internet of Things (IoT) Home Security Systems. HP press release. 10 February 2015, http://www8.hp.com/us/en/hp-news/press-release.html?id=1909050#.VXFusY0w9es.

[28] Lemos, R. Internet of Things security check: How 3 smart devices can be dumb about the risks. PC World. 18 February 2015. http://www.pcworld.com/article/2884612/internet-of-things-security-check-how-3-smart-devices-can-be-dumb-about-the-risks.html.

[29] Boyles, J. L.; Smith, A.; Madden, M. Privacy and Data Management on Mobile Devices. Pew Internet. http://www.pewinternet.org/files/old-media/Files/Reports/2012/PIP_MobilePrivacyManagement.pdf.

[30] Newman, L. H. The internet of things needs anti-virus protection. New Scientist. 12 March 2014. http://www.newscientist.com/article/dn25212-the-internet-of-things-needs-antivirus-protection.html#.VXF1y40w9es.

[31] Rubenking, N. Securing the Internet of Things. PC Mag. 7 May 2015. http://au.pcmag.com/software/30439/feature/securing-the-internet-of-things.

[32] Embedded Security Software & Solutions. http://www.mcafee.com/au/solutions/embedded-security/embedded-security.aspx.

[33] Norton 360 Multi-Device. http://au.norton.com/norton-360-multi-device/.

[34] Host defenses for embedded systems. http://www.redballoonsecurity.com/.

[35] App protection. https://www.arxan.com/products/.