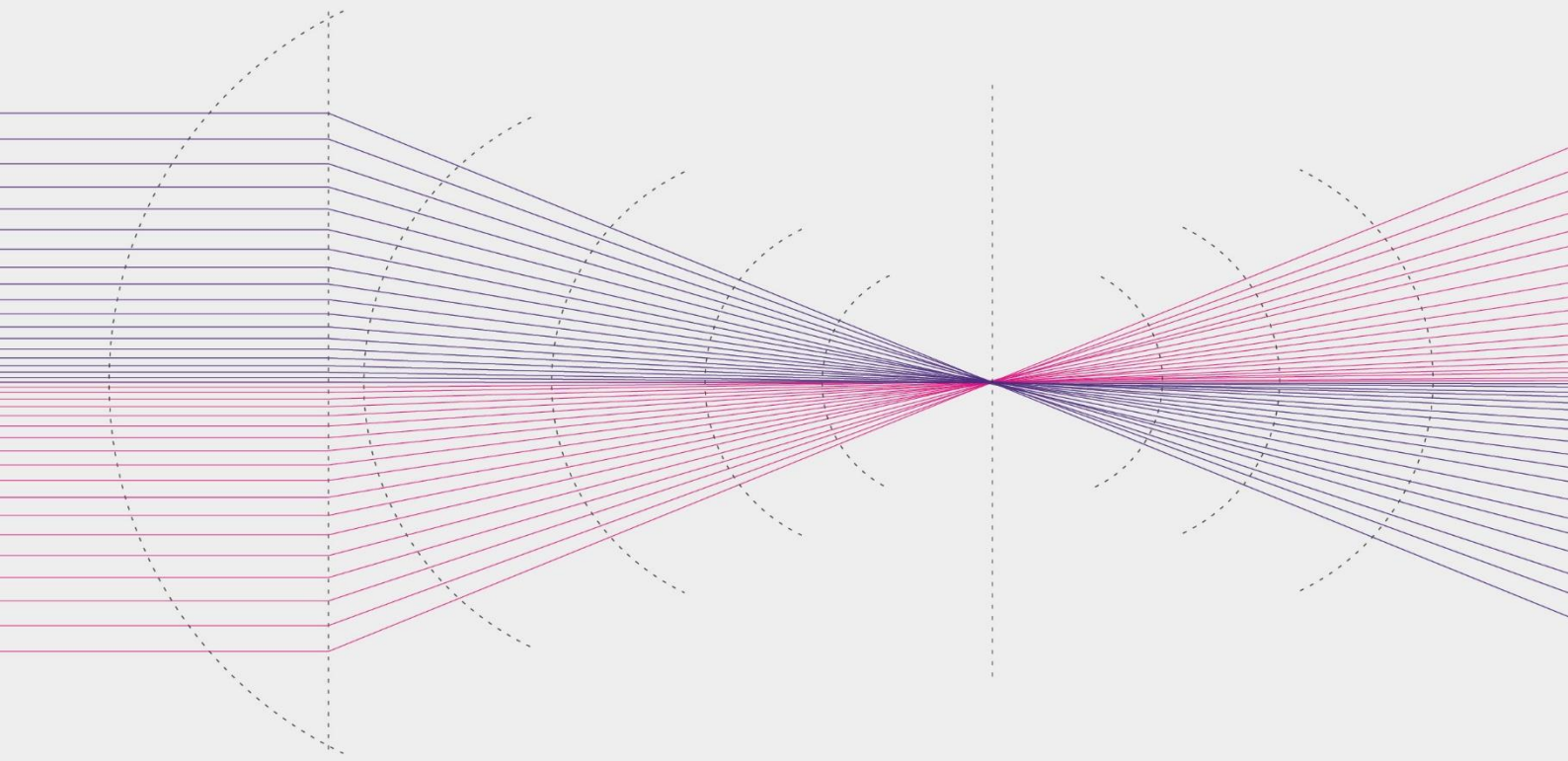
The economics of the security of consumer-grade IoT products and services

April 2019

Mark McFadden, Sam Wood, Robindhra Mangtani, Grant Forsyth



plumconsulting.co.uk

About Plum

Plum offers strategy, policy and regulatory advice on telecoms, spectrum, online and audio-visual media issues. We draw on economics and engineering, our knowledge of the sector and our clients' understanding and perspective to shape and respond to convergence.

About this study

This study for the Internet Society assesses the state of security on consumer Internet of Things devices and the economic factors behind the weak security on many devices. It then draws upon these insights to offer policy recommendations for improving device security.

Founded by the early pioneers of the Internet in 1992, the Internet Society is a global cause-driven organisation working for an open, globally-connected, secure, and trustworthy Internet for everyone. With members, chapters and offices around the world, the Internet Society engages in a wide spectrum of Internet issues – including policy, governance, technology and development – to address the challenges facing the Internet today and to shape its tomorrow.

The authors are grateful for the research inputs contributed by the Internet Society, and for its input in reviewing the report.

Plum Consulting
10 Fitzroy Square
London
W1T 5HP

T +44 20 7047 1919
E info@plumconsulting.co.uk

Contents

© 2019 Plum Consulting

Executive Summary

The Internet of Things (IoT) is a vast network of physical devices – including consumer products, durable goods, cars and trucks, industrial and utility components, sensors and other everyday objects – that have been fitted with Internet connectivity and tools for the collection and exchange of data.

Adding connectivity to physical devices can significantly expand their usefulness: for instance, it can allow remote operation or monitoring of the device, improve user convenience, or enhance energy efficiency. As a result, the number of connected IoT devices has grown rapidly: according to some estimates, the number of IoT devices in operation in 2018 surpassed 10bn.[1]

This growth has been accompanied by increasing concerns about cybersecurity and privacy. Nowhere is this more true than in the consumer IoT segment. This segment – consisting of connected devices intended for personal or residential use, such as smart TVs, connected appliances, voice assistants and home automation devices – accounts for an estimated 63%[2] of the total installed base of connected devices, and is growing quickly.

Security is often lacking in consumer IoT devices: an analysis of 10 of the most common types of consumer devices – including smart TVs, home thermostats, and connected power outlets, door locks and home alarms - found that 70% contained serious vulnerabilities.[3] Potential vulnerabilities include the transmission of unencrypted data over the Internet, insecure software update processes, and the use of non-unique and easily guessable default login credentials.[4]

The exploitation of these vulnerabilities can cause direct threats to the device owner's safety and privacy.[5] For example, in 2015, a researcher reported how he was able to remotely hack into two connected insulin pumps and change their settings so that they no longer delivered medicine.[6] In 2018, a number of connected toys were found to be easily hackable, giving an attacker access to the microphone and location data. And in November 2016, an attack was carried out on a connected heating distribution system in Lappeenranta, Finland, disabling the heating in two buildings.[7]

Insecure devices also present risks to third parties. For example, a compromised device may be enrolled into a botnet – a network of thousands of infected Internet-connected devices under the control of an attacker. Botnets may be used to send spam, distribute malware, commit online advertising fraud, or commit Distributed Denial of Service (DDoS) attacks.[8] DDoS attacks can be used to take websites offline, causing substantial cost to the victim and disruption to users and the wider Internet.

There are a number of technical factors that make consumer IoT devices and services vulnerable to attack. Ultimately, however, weak IoT security has its roots in economic factors rather than technical ones. These include:

[1] https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016
[2] *Ibid.*
[3] Hewlett Packard (2015), *"Internet of Things Research Study"*, http://www8.hp.com/us/en/hp-news/press-release.html?id=1909050 [Hewlett Packard (2015)]
[4] See https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/iot-devices-threat-spreading/
[5] The report's focus is on consumer IoT security rather than privacy; however, privacy issues may be noted where they also relate to security.
[6] FTC (2015), *"Internet of Things – Privacy & Security in a Connected World"*, FTC Staff Report, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [FTC (2015)]
[7] Metropolitan.fi (2016), *"DDoS Attack Halts Heating in Finland Amidst Winter"*, http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter
[8] IBM Security (2016), *"The inside story on botnets"*, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03086USEN

© 2019 Plum Consulting

- **Asymmetric information.** It is often difficult for consumers to discern IoT products with good security from those with poor security. As a result, manufacturers are not rewarded by consumers for investing in effective security measures.

- **Misaligned incentives.** The costs of a security breach of a consumer IoT device or service are borne by the device owner (and wider society), not the manufacturer or service provider. For example, IoT-enabled door and garage locks can be compromised to give an intruder access to a property, but typically the manufacturer does not face the consequences of this intrusion. As a result, manufacturers do not have strong incentives to include effective security in their products and services.

- **Externalities.** Compromised devices can be used to conduct attacks on third parties. This imposes costs on the target of the attack (and on wider society) which are not borne by the device owner, the manufacturer or the service provider. None of these parties will factor these costs into their decision making. This is termed an externality.

As a result of these economic factors, manufacturers are likely to under-invest in security measures. Instead, they will prioritise lowering costs and getting their products to market quickly. Including effective security costs money and slows down the product development process. In addition, it requires specialized skills and experience which manufacturers may not have at hand, requiring either new staff or external consulting – both of which increase costs.

To improve the state of security of consumer IoT devices and services, action will need to be taken to address and compensate for these factors. To be effective, any solutions are likely to require engagement from policymakers and industry. In addition, these solutions will have to strike a balance between improving security and allowing scope for innovation and evolution within the market.

Below we suggest a number of potential actions to address the economic factors. These actions are intended to improve the security of consumer IoT devices and services on the market, and to encourage manufacturers to adopt a 'security-by-design' philosophy, where security is considered at all stages of product development, sale and ongoing support. This set of potential actions has been developed after consideration of a wider number of mechanisms for improving security on consumer IoT devices and services.[9]

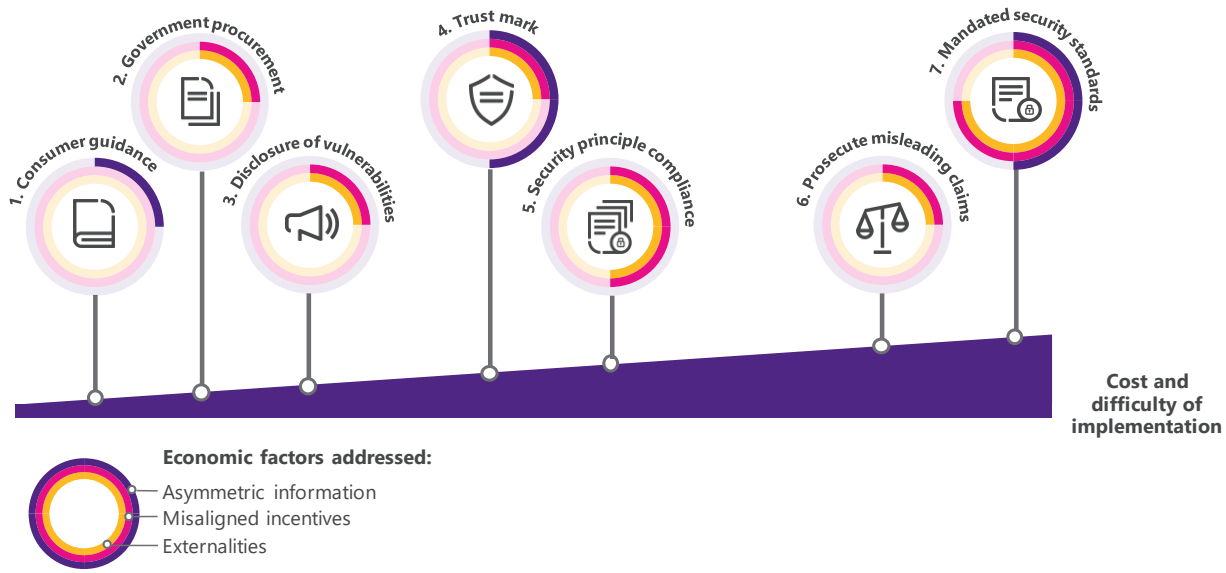
The actions are illustrated in Figure 1. They are listed in order of the likely cost and difficulty of implementing the action. Figure 1 also denotes the efficacy of each action in alleviating (or compensating for) each of the three economic factors behind poor security on consumer IoT: asymmetric information, misaligned incentives and externalities. The actions are aimed at a variety of stakeholders in the market – indeed, actions taken by different stakeholders will complement each other and help drive greater improvements to security. Security measures in the actions are taken to refer to security against both inward and outward threats, in order to protect both the user, third parties and the wider Internet.

It is important to acknowledge that the risk from insecure consumer IoT devices is a global problem: while one country may take steps to keep insecure IoT devices off its domestic market, it will still face risks from insecure devices in other jurisdictions. Growth in connected devices across the world will likely lead to increased transnational liability, security and privacy issues, which existing legal cooperation frameworks may be ill-equipped to handle. Cross-national, regional and global multi-stakeholder efforts to enhance consumer IoT security should be encouraged where possible.

[9] See Section 3 for a detailed discussion of these mechanisms. A subset of mechanisms was selected on the basis that the potential benefits (in terms of improved device security) were likely to outweigh the costs of implementation. From these mechanisms we developed a set of specific, tailored actions for the industry and policymakers to take.

© 2019 Plum Consulting

Figure 1: Potential actions and their efficacy against the economic factors behind poor IoT security



The potential actions are discussed in greater detail below.

1. **Industry bodies and policymakers should prioritise raising awareness of consumer IoT security issues, and provide guidance to buyers.** Providing information to consumers on the possible impacts of insecure devices and the need for them to seek out secure devices and services will empower consumers to make better buying decisions and help correct information asymmetry in the market. For example, in the UK, the Information Commissioner's Office provides such guidance for consumers considering buying IoT products.[10]

2. **Governments should specify a set of security outcomes for their own procurement procedures.** Governments can and should leverage their role as major purchasers to incentivise manufacturers to improve their product. These improvements in security may spill over into the consumer market – it may be easier or cheaper for manufacturers to include the same (improved) security measures in all their products, including consumer products.. The development and documenting of minimum security outcomes could also be the first step in developing a trust mark.

3. **Industry and policymakers should encourage responsible disclosure of software vulnerabilities in consumer IoT.** Policymakers could act to reduce the legal risks faced by security researchers looking to responsibly disclose information on software vulnerabilities they have discovered. Currently such researchers can face legal threats for their actions. Policymakers could create a process for responsible disclosure that reduces the risk that legitimate security researchers will be exposed to legal threats.

4. **The industry should develop a trust mark for secure consumer IoT devices.** A trust mark will facilitate consumers' ability to distinguish between devices at point of purchase, and neatly embodies detailed information. It is also a complement to the awareness raising of publicity about cybersecurity issues. It will assist in resolving information asymmetries in the market, incentivise companies to improve security, and establish an industry process to agree security standards. The trust mark might be based on an existing certification scheme or industry initiative.[11]

[10] Steve Wood (2017), *"The 12 ways that Christmas shoppers can keep children and data safe when buying smart toys and devices"*, Access at: https://ico.org.uk/about-the-ico/news-and-events/blog-the-12-ways-that-christmas-shoppers-can-keep-children-and-data-safe-when-buying-smart-toys-and-devices/

[11] An example of this is the Internet Society's Online Trust Alliance (OTA) IoT Trust Framework.

© 2019 Plum Consulting

5. **Policymakers should require that consumer IoT devices must comply with a set of security principles.** Rather than a rigidly-specified set of prescribed standards, this would involve compliance with various generalised principles – for example, requiring that:

   - the software/firmware on a device can be updated if necessary;
   - the device does not ship with easily-guessable default credentials, or credentials that cannot be changed by the user; and
   - the manufacturer complies with vulnerability disclosure standards.

   This approach should lead to improved device security while retaining flexibility for the market to innovate and improve on security measures.[12] The principles are more likely to remain future-proof (whereas specific encryption methods may eventually become obsolete) and will also apply to new classes of devices.

6. **Policymakers should be more proactive in prosecuting manufacturers or service providers who make misleading claims on security.** This measure would provide an incentive to manufacturers to either improve security or provide honest information about the security on their devices. It could also tie into a wider education/publicity campaign. The US has been active in pursuing device manufacturers that mislead consumers about the level of security on their devices.[13][14]

7. **If the above actions do not result in material improvements in consumer IoT security, regulators could mandate a minimum set of security requirements for IoT devices.** The actions listed above are aimed at improving consumer IoT security without the need for extensive government intervention. However, if industry-led initiatives fail to lead to material improvements in device security, policymakers should be prepared to consider mandating a set of security requirements for consumer IoT, with or without certification.

   This represents a logical extension of Action 5. The main distinction is that, under this approach, the security requirements of a product are much more tightly specified at a technical level – for example, specifying a minimum strength of encryption, or certain criteria for the default credentials (e.g. length). This action could be further reinforced by more rigorous testing of products entering the marketplace to ensure compliance.

   Minimum security requirements may reduce the risk of a device being compromised, and the resultant costs. However, they may also add substantially to the cost of producing and maintaining devices, which could increase prices and reduce adoption (thus decreasing the benefits of connected device adoption for users and wider society) and/or encourage a "black market" in non-compliant devices.

   It is possible that, for some specifications of the minimum security requirement, the costs (in terms of foregone benefits) will outweigh the benefits. It may be difficult to accurately assess these costs and benefits. As a result, it is recommended that this approach is employed only if other measures prove ineffectual.

https://www.internetsociety.org/iot/trust-framework/

[12] In the UK the Department for Culture, Media and Sports (DCMS) offers "Security by Design" recommendations to industry (see https://www.gov.uk/government/publications/secure-by-design). These formed the basis for an ETSI industry standard (see https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf).

[13] In 2017 the Federal Trade Commission (FTC) fined Vizio, a smart TV manufacturer, $2.2m after it was found to be monitoring the operation of its devices without consent https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it

[14] The FTC also filed a complaint that device manufacturer D-Link left its devices vulnerable to hackers, contrary to claims made by D-Link. Though the complaint was dismissed by the court, such actions send a signal to manufacturers that there is the *potential* to be found liable for consumer harm if they mislead consumers on security, helping to address misaligned incentives in the marketplace. https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate

© 2019 Plum Consulting

1 Overview of the consumer IoT market and security

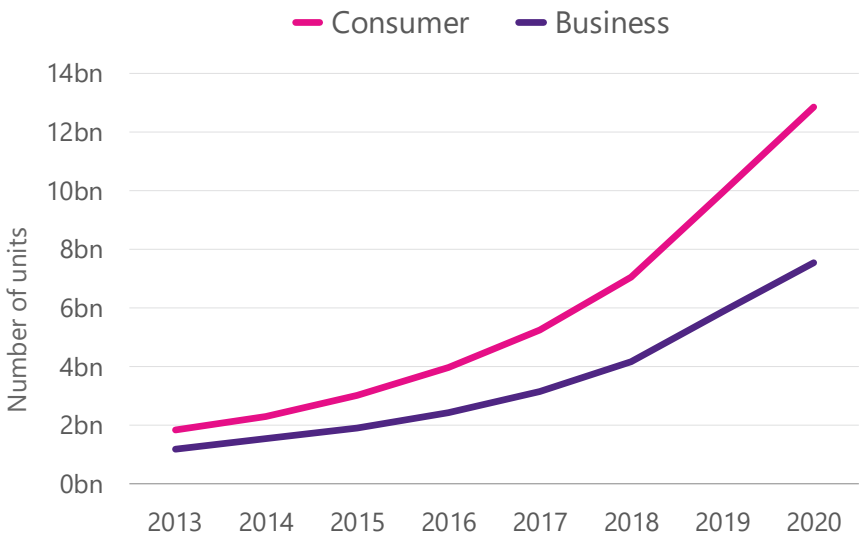
1.1 Size and composition of the consumer IoT market

The consumer IoT market can be divided into three broad categories:

- Home and residential, including smart TVs, smart appliances, voice-activated home assistants, intelligent utility devices, wireless printers and scanners, home automation tools, baby monitors, cameras, door locks and other home security products.
- Transportation, including both in-vehicle and external systems linked to personal transport.
- Health, fitness and personal, including personal safety alarms, healthcare devices, and wearable devices (e.g. Fitbit, Apple Watch, etc.).

Consumer IoT devices comprise the largest share of the total IoT market. According to Gartner, consumer devices (excluding smartphones and tablets) comprised 63% of the total installed base of IoT devices in 2017. As of 2018, the installed base of consumer IoT devices totals around 11bn, and is projected to grow rapidly (Figure 1.1).

Figure 1.1: Installed base of consumer IoT devices



Source: Gartner

The largest segment of the consumer IoT market is Home and Residential IoT devices. The dominant consumer IoT device, worldwide, is the smart TV. Between 25-35% cent of consumers worldwide own a television that can connect to the Internet.[15]

Beyond smart TVs, the remainder of the Home and Residential IoT category is still nascent, but growing rapidly. Other devices included in the segment include: smart speakers and voice assistants, home automation devices,

[15] Deloitte (2017), *"Global Mobile Consumer Trends"*, https://www2.deloitte.com/ng/en/pages/technology-media-and-telecommunications/articles/global-mobile-consumer-survey.html

© 2019 Plum Consulting

security devices, and smart appliances, garden equipment and toys. Many of these devices are relatively inexpensive. See Appendix A for a wider description and discussion.

1.2 Security in the consumer IoT market

The growth in the IoT marketplace has created many opportunities for innovation, but has also led to new risks. A study by Hewlett Packard in 2015 found that 70% of the most commonly used IoT devices contain serious vulnerabilities.[16] The security of IoT devices, services and systems can be tested in four key dimensions:

- confidentiality of data;
- integrity and authentication of device connections;
- control and availability of device to connection requests; and
- capability of device to participate in attacks.

In a 2017 study[17] 20 consumer IoT devices were tested in these four dimensions on a three-tier rating scale of "secure," "moderately secure," to "insecure." They found that all devices tested had shortcomings in one of the four dimensions.

The research also indicates that the security risks are growing with the market. Symantec reported a 600% increase in attacks against IoT devices from 2016 to 2017.[18] Estimates show that about 4,000 new vulnerable IoT devices become active each day.[19] In Autumn 2017, a list of IP addresses and login credentials (many of them the combination "admin/admin") for more than 8,000 Telnet-accessible consumer IoT devices was posted on Pastebin.[20]

1.3 Why are consumer IoT devices vulnerable?

There are a number of technical factors behind the vulnerability of consumer IoT devices to attacks. Some of the main factors are listed below.

- The use of easily guessable default credentials – Shipping tens or hundreds of thousands of the same device with a unique password on each adds to production costs. Most IoT home devices that employ some level of authentication often ship with the same default credentials, which are often easily guessable and seldom changed by the end-user (this was one of the reasons the Mirai botnet grew so large so quickly).
- Weak security at the software level – Many products are not designed securely. Web interfaces of devices are prone to a variety of issues such as persistent cross-site scripting, poor session management, and weak default credentials. Some devices also do not encrypt network services transmitting data via

[16] Hewlett Packard (2015), *"Internet of Things Research Study"*, http://www8.hp.com/us/en/hp-news/press-release.html?id=1909050 [Hewlett Packard (2015)]
[17] F. Loi, et al (2017), *"Systematically Evaluating Security and Privacy for Consumer IoT Devices"*, proceedings of the 2017 Workshop on Internet of Things Security and Privacy, IoTS&P '17 pp.1-6, 2017
[18] Symantec (2018), *"Internet Security Threat Report – Volume 23 (March 2018)"*, https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf [Symantec (2018)]
[19] James Scott and Drew Spaniel (2016), *"Rise of the Machines: The DYN Attack was just a Practice Run"*, CreateSpace, ISBN-13: 978-1540894571
[20] See https://arstechnica.com/information-technology/2017/08/leak-of-1700-valid-passwords-could-make-the-iot-mess-much-worse/

© 2019 Plum Consulting

the Internet and local network.[21] IoT devices may come from the manufacturer with vulnerabilities in the form of number of services and ports that are open by default.[22]

- The use of outdated software and lack of software updates - Many consumer IoT device manufacturers do not issue prompt or regular updates for the software on those devices. Even when updates are issued, the end-user may not be informed, or may not have enough technical know-how to install the update. End-users are also unlikely to periodically check for and install updates on their various IoT devices. Perhaps more troubling is that many consumer IoT devices don't have a way to be updated at all.[23]

- Lack of a secure update mechanism – It is essential is that software updates come from a trusted and authentic source (where the source of the update is properly authenticated) and that the update cannot be tampered with in transit (the contents of the update are encrypted). However, many firmware update functions in IoT home devices have been shown to be exploitable in ways that allow attackers to upload modified, malicious versions of the firmware – for example, by not encrypting the update. In many cases, the user is unlikely to be aware of this.

- Limited user interface – Many IoT consumer devices lack the luxury of a full screen and keyboard interface for interaction, requiring intuitive use of minimal buttons or actions for operation. Embedding security controls into such restricted interfaces can be difficult and may be detrimental to the device's functionality or ease of use, and so is commonly omitted. A limited user interface may also make it harder for users to change the default password.

- Small form factors and limited capability components – Many IoT home devices are designed to be as small as possible and often comprise components with limited capability. For example, chipsets and memory have weak upper limits on the strength of encryption that they can support. These upper limits may not be (and commonly are not) in line with current best practice and are exploitable through known and existing vulnerabilities. If chipsets are not powerful enough to handle the data processing required, the data needs to be transmitted (and often the transmission is not secure).

- Rush to market means little time for testing – Products are commonly released having undergone little to no security assurance testing.

1.4 Nature of risks from insecure consumer IoT devices

Poorly-secured IoT products and their associated services pose both direct risks to the consumer ("inward risks") and to the wider Internet ("outward risks"). These risks are discussed below.

Inward risks

Poorly-secured IoT products and their associated services can directly threaten individuals' online security, privacy and safety. For example:

- a home with smart locks that have been compromised could allow criminals to have access without forcing entry;

[21] Hewlett Packard (2015).
[22] See https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/iot-devices-threat-spreading/
[23] For example, many of the devices compromised by the Mirai botnet cannot be updated to protect against the attack.

© 2019 Plum Consulting

- compromised consumer IoT devices connected to home heating or "smart appliances" can cause safety risks: an attacker might be able to disable safety controls or deny usage, such as disrupting heating systems in winter;

- devices with microphones or cameras, which can be compromised to allow home voice recordings and images to become publicly available for those wishing to access them;[24]

- devices with presence or location-tracking capability can be used to record and extract information about consumer's daily routine or used to exploit, harass or blackmail the user.

Moreover, just a single compromised IoT device can be used to facilitate attacks on the consumer's network and other devices on that network.[25]

Outward risks

In addition to inward risks to the consumer, compromised IoT devices can be used to spread malware or launch attacks on a third party. Compromised devices may be recruited into a 'botnet' – a network of thousands or millions of infected Internet-connected devices under the control of an attacker.[26] Botnets may be used to send spam, steal user credentials, distribute malware, commit online advertising fraud, mine cryptocurrency or commit a Distributed Denial of Service (DDoS) attack.[27]

These types of attack can cause substantial harm at a local, national or even international scale. The foregone revenue to firms faced with such attacks – just one dimension of the costs of an attack – can reach into hundreds of thousands of dollars.[28] Perhaps the most famous example of a large-scale attack using IoT devices is the Mirai botnet, which, in a large-scale attack on domain name server (DNS) provider Dyn knocked dozens of sites offline for a day – including Amazon, Spotify, and Twitter. Reportedly, around 8% of Dyn's customer base stopped using its services in the wake of the attack.[29]

A growing concern is that the full power of a botnet could be leveraged to attack critical national infrastructure. For instance, Symantec has noted that some attack groups are probing energy network infrastructure.[30] A large-scale attack against critical infrastructure has the potential to cause enormous disruption and large costs to society.

See Appendix B for a detailed discussion on the inward and outward risks associated with vulnerable devices and services, the financial investment in IoT security, consumer attitudes and market developments in IoT security.

[24] For example, in 2017 this occurred with connected toys. See http://www.bbc.co.uk/news/technology-39115001
[25] FTC (2015), *"Internet of Things – Privacy & Security in a Connected World"*, FTC Staff Report, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [FTC (2015)]
[26] ENISA (2018), *"Threat Landscape Report 2018"*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
[27] IBM Security (2016), *"The inside story on botnets"*, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03086USEN
[28] https://www.akamai.com/us/en/multimedia/documents/content/ponemon-institute-the-cost-of-ddos-attacks-white-paper.pdf
[29] https://www.corero.com/blog/797-financial-impact-of-mirai-ddos-attack-on-dyn-revealed-in-new-data.html
[30] http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf

© 2019 Plum Consulting

2 Economic factors behind poor consumer IoT security

Given the potential costs and consequences of the types of security incidents discussed above, and consumers' concerns over the security of connected devices, several questions arise. Why are consumer IoT devices with weak security commonplace? Why are consumers buying them? And why aren't device manufacturers investing in better security, and winning market share by doing so?

These questions can be answered by identifying the economic (rather than technical) factors behind weak consumer IoT device security: information asymmetries, misaligned incentives and externalities. The presence of these factors results in underinvestment in consumer IoT device security, and explains why consumer IoT manufacturers and service providers lack the incentive to improve the security of their products. Each of these factors is discussed in more detail below.

In addition, studies in behavioural economics – an area of research that fuses economics and psychology – indicate that consumers may not behave rationally, even when they have enough information to make the 'right' (i.e. welfare-maximising) decision. These insights will be important for understanding why consumers buy insecure products and when considering the efficacy of various actions to improve security in consumer IoT devices and services.

2.1 Information asymmetries

Information asymmetry refers to a situation in which one party to an economic transaction has more information than another. This normally (though not always) occurs when the seller of a good or service has more knowledge than the buyer. In such a case, the result is downward pressure on both price and quality, leading to a market failure.

In 1970, economist George Akerlof illustrated the concept with reference to the used car market.[31] The example runs as follows: imagine a town with 50 good used cars for sale (worth $3000 each), and 50 "lemons" – unreliable used cars – worth $1000 each. The sellers know which type of car they have but the buyers do not.

If customers believe there is an equal chance they will get a good car or a lemon, they might initially offer $2000. But no seller is willing to sell a good car for that price, so the market price drops to $1000, with only lemons being sold. The key insight is that buyers are unwilling to pay a premium for quality they can't measure, creating a disincentive to supply high-quality products.

This concept was being applied to information security as early as 2001,[32] and has been discussed in numerous cases since. For example, a study on the prevalence of fake anti-virus software suggests that many consumers have trouble distinguishing the "lemons" from the good products.[33] Moreover, as the technical complexity of products on the market increases, problems of information asymmetry are likely to worsen.[34]

There is often no easy way for a consumer to assess, prior to purchase, the level of security offered by a consumer IoT device or service. Often, little information on the included security measures is provided before

[31] George A. Akerlof (1970), "*The Market for "Lemons": Quality Uncertainty and the Market Mechanism*", The Quarterly Journal of Economics, Vol. 84, No. 3. (Aug., 1970), pp. 488-500.
[32] Ross Anderson (2001), *"Why Information Security is Hard – An Economic Perspective"*, Seventeenth Annual Computer Security Applications Conference, 10-14 Dec. 2001, https://www.acsac.org/2001/papers/110.pdf
[33] Brett Stone-Gross et al (2011), *"The Underground Economy of Fake Antivirus Software"*, WEIS 2011.
[34] Michelle Baddeley (2011), *"Information Security: Lessons from Behavioural Economics"*, Conference: Security and Human Behavior 2011 (SHB11) [Baddeley (2011)]

© 2019 Plum Consulting

purchase. Even when it is, the technical terminology involved, for example, around encryption standards, many not be familiar to many users.

In any case, a consumer IoT device or service that claims to be secure and to employ strong encryption schemes may not actually be secure in practice. For example, ZigBee, a popular IoT standard, uses a strong encryption and authentication scheme, but attackers have still been able to take control of ZigBee-certified products.[35,36] All in all, this makes it highly challenging to assess, in practical terms, exactly how secure a device will be once it is connected and in use.

In addition, the consumer is rarely provided with information on product aftercare: the regularity of updates, the speed with which security holes will be patched, and the duration of ongoing device support.

2.2 Misaligned incentives

Consumer IoT device manufacturers and service providers have little incentive to improve security measures. In part this is because consumers will not always reward them for doing so (see Section 2.1), but also because the companies do not bear the full costs of security breaches on their products.

As discussed previously, due to the diverse nature of the consumer IoT market, a security breach could have wide-ranging implications and costs for the user. including potential identity theft, fraud and the harm to property or personal security.

Yet as device manufacturers and service providers do not bear these costs, they lack the incentive to improve security. This leads to a situation of misaligned incentives between manufacturers and consumers: the party making the security-efficiency trade-off is not the one who loses out when attacks occur.

Instead, device manufacturers are rewarded for reducing costs, adding product functionality, and being first to market. Security testing and implementation generates additional costs and delays in reaching the market – and both erode profits. More effective security measures may also reduce product functionality and ease of use, which could make the product less attractive to consumers.

Given many consumer IoT devices are inexpensive and essentially disposable, profit margins may be tight, and it may be uneconomic for manufacturers to invest in device security. Moreover, many consumer IoT devices are made by companies without prior experience in software development, and which lack in-house capability in information security.[37] In addition, suppliers – particularly those developing low-end devices – lack economic incentives to provide ongoing support or security updates after purchase, leaving consumers with unsupported or vulnerable devices.

2.3 Externalities

A compromised IoT device, service or system imposes costs not only on the user, but on the wider Internet ecosystem. For example, if a device is compromised and becomes part of a botnet, it can be used to launch

[35] Philipp Morgner and Zinaida Benenson (2018), *"Exploring Security Economics in IoT Standardization Efforts"*, Workshop on Decentralized IoT Security and Standards (DISS) 2018 18 February 2018, San Diego, CA, USA, https://dx.doi.org/10.14722/diss.2018.23009

[36] Eyal Ronen et al (2017), "*IoT Goes Nuclear: Creating a ZigBee Chain Reaction*" 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2017, pp. 195-212. https://ieeexplore.ieee.org/document/7958578/

[37] Consumers International (2016), *"The Internet of Things and challenges for consumer protection"*, https://www.consumersinternational.org/media/1292/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf pp.32

© 2019 Plum Consulting

DDoS attacks, to send spam, propagate malware or to host phishing scams, contributing to wider Internet insecurity.

The costs of such attacks can be substantial, but in many cases, the attack target is someone other than the device owner (indeed, the owner may even be unaware their device has been compromised). The insecurity in the device imposes costs on the target of the activity (and on wider society) which are not borne by the device owner. In economics terminology, these effects are referred to as negative externalities.

Negative externalities pose a problem insofar as neither the IoT supplier nor the consumer will factor the wider impact of device insecurity into their decision-making. As discussed in Sections 2.1 and 2.2, suppliers are not incentivised to improve device security; their objectives are primarily reaching the market quickly and cost-effectively. Device owners, meanwhile, will be less inclined to spend time setting up and patching devices (or learning how to do this) if attacks do not harm them directly.

As network security is a collective responsibility, leaving its provision to the unregulated market or individual will tend to result in its under-provision, to the detriment of society as a whole.[38] Consumers and companies will be tempted to "free-ride" on others' investments in network security measures, without bearing any of the costs themselves[39] (secure devices generate positive externalities, in the form of a safer and more secure Internet for all users).

Lastly, there is the risk that poor security on these devices means that positive externalities are foregone. 'Scare stories' about the IoT may deter device adoption, even though these devices could provide significant benefits to the user and positive externalities to society (for example, the adoption of energy-efficient smart devices could reduce society's electricity consumption). A survey of 2,000 consumers found that one in five claimed to have been put off buying smart home devices in the wake of recent IoT security issues.[40]

[38] Wendy Seltzer (2014), *"Network Security as a Public Good"*, https://www.w3.org/2014/strint/papers/60.pdf
[39] Baddeley (2011).
[40] Canonical for Ubuntu (2017).

© 2019 Plum Consulting

Figure 2.1: Explaining consumer behaviour with behavioural economics

The discussion of the economic factors has thus far assumed a rational choice approach (albeit one with imperfect information). Such an approach assumes that individuals make rational choices to maximise their welfare, given the information available to them.

However, behavioural economics indicates that individuals' cognitive biases and limitations affect their decision-making. In particular, individuals often rely on heuristics – rules-of-thumb or mental shortcuts – to make decisions, even when they have the information to make a 'rational' choice. Heuristics are particularly relevant when a full assessment of the available information is difficult or time-consuming.

Several cognitive biases are likely to be relevant when consumers are making judgements about information security:

- The availability heuristic represents the ease with which an idea can be brought to mind. Consumers may, for example, decide security is not a problem because it hasn't been a problem in the past.[41]
- The anchoring heuristic suggests the value individuals attach to things is affected by context. For example, the value attached by a user to privacy has been found to be highly sensitive to the context in which they are asked for information.[42]
- Individuals find it hard to assess low probabilities, which may lead them to be overoptimistic about future events and sanguine about their vulnerability to privacy violations or being hacked.[43,44]
- Individuals are often time-inconsistent. This may lead them to procrastinate about setting up effective security measures.[45]

These insights may go some way toward explaining the paradox discussed in Section 3.4: that consumers have concerns about the security of IoT devices but still buy them (and, in many cases, don't take basic security precautions). These considerations should be factored in by policymakers when considering potential remedial measures that require user action.

[41] Baddeley (2011).
[42] Alessandro Acquisti, Leslie K. John, and George Lowenstein (2013), *"What is privacy worth?"*, Journal of Legal Studies, vol.42 (June 2013).
[43] Baddeley (2011).
[44] Alessandro Acquisti and Jens Grossklags (2005), *"Privacy and rationality in individual decision making"*, IEEE Security & Privacy Volume 3 Issue 1, January 2005. https://dl.acm.org/citation.cfm?id=1048819
[45] Alessandro Acquisti and Jens Grossklags (2006), *"What can behavioural economics teach us about privacy"*, Presented as Keynote Paper at ETRIC 2006. https://www.heinz.cmu.edu/~acquisti/papers/Acquisti-Grossklags-Chapter-Etrics.pdf

© 2019 Plum Consulting

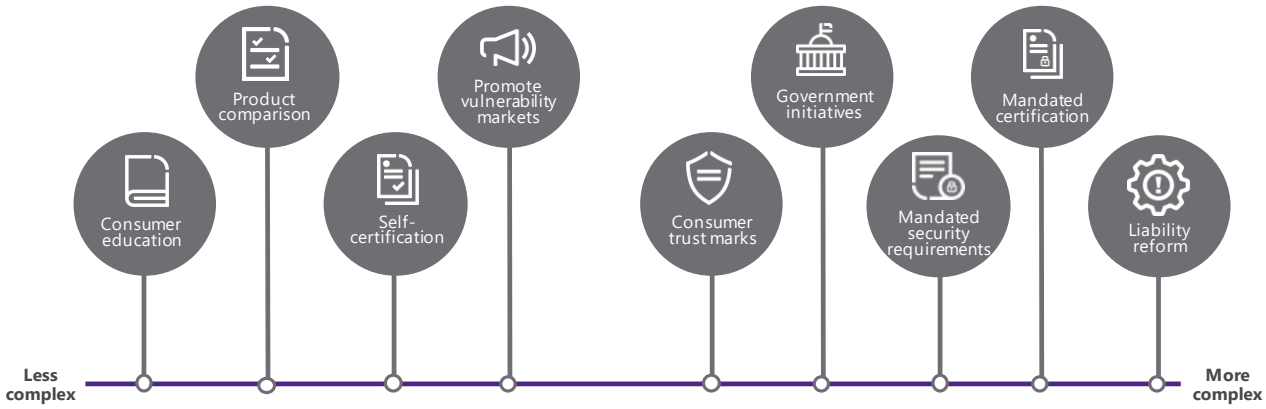
3 Potential mechanisms for improving consumer IoT security

3.1 Taxonomy of mechanisms

This section discusses different mechanisms that could be employed to improve the security of consumer IoT. They have been chosen because they reflect measures that are commonly advocated, or have been adopted in this or other industries. This is not intended to be an exhaustive list of all potential mechanisms for improving consumer IoT security; rather, it is to focus the analysis on the most widely-discussed measures.

Broadly, the mechanisms can be characterised by the degree of complexity involved in their implementation (Figure 3.1). The more complex mechanisms generally involve a greater degree of intervention into the consumer IoT market, but may also be more effective at delivering improved security. It is possible for several different mechanisms to be deployed in concert.

Figure 3.1: The mechanisms discussed



The following sections outline the pros and cons of each mechanism in delivering improved security. It should also be kept in mind that security on the open Internet is a global challenge; unilateral actions by one nation will not eliminate the threat to that nation posed by insecure IoT devices in other nations.

3.2 Consumer education

Consumer education initiatives involve providing consumers with better information on IoT security principles, problems, and terminology. Several governments around the world have already launched campaigns (such as the UK's £4m 'Cyber Aware' campaign) to encourage consumers to be more cyber-aware in their use of connected devices.

Such campaigns may help to resolve the information asymmetries in the market by providing consumers with the knowledge to make more informed product choices. Moreover, by raising awareness of the risks, consumers may be more motivated to take measures to secure their devices. However, a major challenge of education campaigns is reaching and engaging consumers. Campaigns must provide sufficient information to allow consumers to make informed choices without overloading them with technical detail. This may be a difficult balance to strike.

© 2019 Plum Consulting

Education is also a somewhat reactive solution to security issues, and will not address the introduction of fundamental vulnerabilities at the device, service and network level. Vulnerable devices will still be available on the market, and those devices will pose a risk to the systems of others. It will likely be difficult to motivate even informed consumers to spend their time and money securing their devices if the main victim of an attack is someone else.[46] In addition, any education programme needs to account for the fact that consumers may not always react as expected in the face of a cyber threat (see Figure 2.1).

3.3 Product reviews and comparisons

Product reviews, ratings and comparisons can assist consumers in making purchasing decisions. They are particularly relevant for products with complex functions or where product attributes may conflict – such as security and ease of use. Authoritative information sources, such as comparison reports produced by respected consumer advocacy organisations, independent technology reviewers and certified comparison websites, can help consumers make more informed choices, helping to resolve information asymmetries in the market. In turn, this should provide incentives for suppliers to improve security measures on their devices, to avoid the negative publicity generated by negative reviews.

However, there are limitations to what product reviews and comparisons may achieve. First, unless the reviewer is a security expert, they may not fully review a product's security – for example, whether it uses a secure update process. Insecure products may therefore still receive positive reviews. Second, reviews and comparisons tend to be local in reach, and will only be effective for the subset of consumers that conduct research prior to purchase. Finally, like consumer education programmes, negative product reviews will not remove insecure devices and services from the market.

3.4 Vulnerability disclosure and vulnerability markets

Vulnerabilities are flaws or weaknesses in a system's software that can be exploited by an attacker to compromise the security of that system and cause loss or harm. Vulnerability discovery, management and patching are vital for keeping a connected product or service secure throughout its lifecycle.

Vulnerabilities may be discovered by individual security researchers or by organisations. Once a vulnerability is found, the finder can disclose the vulnerability to the vendor, publicise it or sell it on the 'grey market' – consisting of groups and organisations that may use the information for a variety of purposes (for example, for penetration testing, or to conduct attacks).

Many companies offer rewards or "bounties" for the disclosure of vulnerabilities. Both the number of disclosures and the rewards offered by companies have increased in recent times.[47] But in spite of this growth, researchers can often run into legal challenges when investigating or disclosing vulnerabilities. These can include not only criminal law challenges, but also – depending on the methods used – contract, licensing, copyright and patent law.[48] These can discourage vulnerability detection and responsible disclosure.

Once disclosed, vulnerabilities are commonly fixed by the issuance of a patch. However, some vendors – particularly those without an established brand or reputation – may simply not be motivated to correct a vulnerability, promptly, if at all. For example, tech firm Xiongmai neglected to fix the security flaws in its

[46] This is generally the case for DDoS attacks. See Section 2.3 for discussion of this issue.
[47] Abdullah Algarni, and Malaiya Yashwant (2014),"*Software vulnerability markets: Discoverers and buyers.*" International Journal of Computer, Information Science and Engineering 8.3 (2014): 71-81.
[48] ENISA (2015).

© 2019 Plum Consulting

consumer IoT devices, despite knowing about them for seven months.[49] Nevertheless, vulnerability discovery and reward schemes are generally perceived as a positive development in the field of information security.[5051]

3.5 Self-certification and voluntary codes of practice

Industry self-regulation of privacy and security for consumer IoT devices has been proposed as a flexible alternative or complement to the imposition of traditional regulation. There are a variety of self-regulatory models in place, including trade association memberships (for instance in the marketing industry with the Digital Advertising Alliance), certification programs (such as TRUSTe), or co-regulatory frameworks (such as the UK's Advertising Standards Agency). Such programs are usually voluntary.

For Internet-based technologies (especially in the area of privacy) voluntary, self-certification has not been particularly successful in improving privacy or security outcomes. Academic research on self-regulation and voluntary standards in other industries – such as financial, environmental, healthcare, food and others – finds mixed results as to the efficacy of self-regulation.[52]

Self-regulation is a common response to the perceived threat of governmental regulation. In 2018, the IoT Alliance Australia (IoTAA) prioritised the introduction of an 'IoT product security certification program' as a part of its strategic plan. Exactly what this will look like remains unknown, but it is likely to be performed by accredited independent bodies that evaluate products based on security claims.

Self-regulation may help to improve security on compliant devices, and to promote a security-by-design philosophy among manufacturers. However, some manufacturers may simply elect to remain outside the self-regulation scheme to keep their costs and prices low. This would undermine a self-regulatory scheme and could exacerbate information asymmetry in the market by adding to consumer confusion. A self-regulatory regime may also be prone to 'gaming' by manufacturers, who may seek to set any standard at an easily achievable level which may only marginally improve security.

3.6 Trust marks and labels

It is common for consumer products to be tagged with certain labels and trust marks. Trust marks are usually symbols that range from indicating danger to how the product should be recycled. Labels usually provide more detailed information in the form of written text, tables and scales. In technology, simple labels are commonly employed – for example, the padlock icon to indicate TLS secure connections, or the green tick used to verify certificates or URIs. Such schemes could be extended to Consumer IoT devices with limited screens to indicate, for instance, that the device is connected to a trusted gateway or hub.

There is academic research that shows that labels can be successful in guiding consumer behaviour. For instance, studies on the influence of energy efficiency labels indicate that consumers not only are aware of the labels, but that they understand them and allow the labels to influence their purchasing decisions.

One approach is to legislate for security labels on consumer IoT devices. For example, such labels could indicate the security lifetime of the product (how long the manufacturer will provide security updates for the product)

[49] See https://krebsonsecurity.com/2018/10/naming-shaming-web-polluters-xiongmai/

[50] Mingyi Zhao, Jens Grossklags and Peng Liu (2015), *"An Empirical Study of Web Vulnerability Discovery Ecosystems"*, Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM https://s2.ist.psu.edu/paper/An-Empirical-Study-of-Web-Vulnerability-Discovery-Ecosystems.pdf

[51] ENISA (2015).

[52] See, for example Murdoch, Bond and Anderson (2012), *"How certification systems fail: Lessons from the Ware report,"* IEEE Security & Privacy, vol. 10 no.6, pp. 40-44, or Leverett, Clayton, and Anderson (2017), *"Standardization and certification of the 'Internet of Things'*," 16th Annual Workshop on the Economics of Information Security, WEIS 2017, University of California, San Diego, CA, USA.

© 2019 Plum Consulting

and the maximum time-to-patch (how long the manufacturer will take to address security flaws in the event of vulnerabilities being identified).

Another approach is a voluntary trust mark, absent legislation, which could be self-asserted or externally audited. This would need to be accompanied by a substantial and long-term publicity campaign to raise public awareness. While an externally audited trust mark is clearly stronger and more meaningful, the cost burden on manufacturers could be substantial and thus some might choose the self-asserted version even if offered a choice.

Labelling and trust marks for IoT devices have advocates: governments and consumer groups have been enthusiastic about trust marks and labels because of their success in other sectors of the market.[53] Recent research attempts to combine existing strategies for labelling from these other sectors with solutions to problems identified by the IoT device manufacturers and service providers.[54] Success in other verticals (for instance, eHealth or Intelligent Transportation Systems) might also lead to trust marks getting greater acceptance in consumer settings.

However, as the IoT industry is far more fluid than the food or appliance industries, it may be challenging to set up a trust mark that was flexible enough to address new products, services and devices in the market.[55] Moreover, a product label that specifies that security characteristics of an individual device might not give any information about how that device performs, in respect to security, in the presence of other devices.[56]

3.7 Other government initiatives

There are a number of potential actions governments could take in order to promote better security on consumer IoT devices. For example, a government might:

- create a code of practice or guidelines to encourage improved security, for example, the UK's Secure by Design initiative;[57]
- require that government and public procurement only considers devices and services that meet certain security standards;
- offer financial incentives[58] to consumers purchasing devices and services that meet a set of security standards; or
- offer tax breaks (or other inducements) to companies whose products meet a set of specified security standards.

These initiatives would reward manufacturers for producing devices with better security by encouraging the production and purchase of secure devices. As a result, they may help resolve problems of information asymmetry in the market (by helping to push consumers towards buying more secure devices), and to correct for the negative externalities generated by insecure devices.

[53] For example, the European Commission is interested in a trust mark that could be applied to IoT devices. This approach would specify an appropriate level of security for products and services, which must be met in order for a product to receive the trust mark. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity
[54] https://ieeexplore.ieee.org/document/7845514/
[55] https://www.bna.com/companies-wary-eu-n57982083682/
[56] Scott Peppet (2014), "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent", Texas Law Review 93(1): 85-176.
[57] See https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security
[58] Similar to schemes like export incentives, car scrappage schemes, or funding for innovative activity.

© 2019 Plum Consulting

However, there are some challenges in implementing such initiatives. The government would be required to define 'acceptable' security standards for consumer devices. If these standards are too lax, the problem is not resolved; if they are too high, the costs – in terms of higher device prices and lower adoption – may not outweigh the benefits (requiring 'perfect' security on all devices is unlikely to be economically optimal[59]).

Similarly, it would be challenging to determine the appropriate level for a rebate (or tax break or subsidy). This would need be sufficient to induce some consumers to switch to purchasing devices with better security (and to compensate for the negative externalities of insecure devices[60]). However, attempting to estimate the costs – in monetary terms – of connecting an insecure device to a network is likely to be extremely complex.

Determining eligibility and how rebates or subsidies are administered is also likely to be a challenge – such a scheme may be prone to 'gaming' by manufacturers and vendors. In addition, not all governments have equal weight in influencing the market – governments of smaller nations may find it more challenging to influence the behaviour of the market using the above measures.

3.8 Mandated security requirements

A policymaker or a regulator could introduce a set of legal requirements obliging a manufacturer's products to meet a minimum level of security. This is not an unusual approach in other industries – such as health care or the automotive industry. In some cases, there are internationally harmonized common rules, but it is also common for standards to be set on a national or regional basis.

The extent and impact of such a regime depends on how comprehensive the requirements are. Regulators might require:

- certain technical standards to be met, for example setting certain encryption standards, or requiring a unique pre-programmed password on each device;[61]
- adherence (whether self-asserted or externally certified) to a known and trusted set of security guidelines;[62]
- a secure product lifecycle, indicating that a device be supported or patched for a certain duration; or
- the adoption of certain procedures for vulnerability disclosure or patching.[63]

Mandated security requirements might be enforced by ex-post action by the regulator, or via a self-certification regime. Alternatively, manufacturers might be required to have their products certified by an independent body or testing agency (discussed further in Section 3.9).

While mandating a certain level of security can help stop products with poor security reaching a market and provides more flexibility for manufacturers and service providers to identify the tools that most meet their security needs, there are challenges in this approach. Minimum security requirements may add to the cost of

[59] Tyler Moore (2010), *"Introducing the Economics of Cybersecurity: Principles and Policy Options"*, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy [Moore (2010)]

[60] A Pigovian tax is a tax applied to goods that generate negative externalities, in an attempt to deter consumption. Conversely, a Pigovian subsidy (similar to what is proposed here) attempts to encourage consumption of goods that generate positive externalities (i.e. secure devices).

[61] The latter requirement was part of a recently enacted law in the State of California concerning the security of connected devices. See: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

[62] An example of this is the Internet Society's Online Trust Alliance (OTA) IoT Trust Framework https://www.internetsociety.org/iot/trust-framework/

[63] Leverett, Clayton and Anderson (2017) point out that there is now an ISO standard for vulnerability disclosure. They suggest that this might be used to hold companies to account if their devices cannot be patched.

© 2019 Plum Consulting

producing devices, which could increase prices and reduce adoption (thus decreasing the benefits of connected device adoption for users and wider society).[64]

It is possible that, for some specifications of the minimum security requirement, the costs (in terms of foregone benefits) will outweigh the benefits. The agency supervising the mandatory requirements must develop and set those requirements, but it may prove difficult to accurately assess the costs and benefits and set the minimum requirements at the economically-efficient level. In addition, such a measure would only impact the risk from connected devices in the domestic market – not those in other jurisdictions.

Further, since the market is developing, these requirements will need to be frequently updated. The regulator must also monitor the market and ensure action is taken against manufacturers and vendors that do not comply with the security requirements. Further, it may prove difficult to prevent the importation of devices from other jurisdictions where there are no such requirements. Nevertheless, mandating security requirements may prove helpful in dealing with the most egregious security flaws, for example, devices that cannot be patched. It would also help improve the security on new classes of devices, which may not be covered by other pre-existing regulations or standards.

3.9 Mandated certification

A regime of mandated security requirements may be further reinforced by a requirement on manufacturers and vendors to certify that their products meet those requirements. This might involve:

- security testing by an independent testing laboratory, for example a Common Criteria Testing Laboratory;[65] or
- testing and certification by a government agency or a public-private agency.

Mandated certification adds an additional level of surety that a device is actually compliant with mandated security requirements. However, testing and certification of devices is expensive, and may increase costs or device prices. Device testing may also be prone to 'gaming' by device manufacturers – for example, they may choose testing labs that will give their product an easy ride. Testing labs may also be less than thorough in their testing, allowing devices with weak security to gain accreditation.[66]

3.10 Liability reform

Liability reform would attempt to evolve liability laws so that IoT manufacturers, suppliers and/or retailers are held liable for the damages caused by wilful or negligent poor security on their devices and services. Effecting such reform could resolve the problem of misaligned incentives in the market, as suppliers would be obliged to face the consequences of poor security on their products.

Regulatory intervention can seek to achieve this, although few regulatory environments are currently set up with the authority to impose penalties for poor security or ban the sale of insecure consumer IoT. However, in 2017,

[64] These might include, for example, the use of smart thermostats and home management systems, generating costs savings for the user and environmental benefits for society.
[65] A Common Criteria laboratory is a third-party security testing facility that is accredited to conduct security evaluations for conformance to the Common Criteria international standard.
[66] Steven J. Murdoch, Mike Bond and Ross Anderson (2012), *"How Certification Systems Fail: Lessons from the Ware Report"*, IEEE Security & Privacy, volume 10, issue 6, pages 40–44, Nov–Dec 2012.

© 2019 Plum Consulting

the German regulator, Bundesnetzagentur, banned the sale of the Cayla doll because it could be used a surveillance device.[67][68]

Assigning liability to manufacturers, suppliers and/or retailers for wilful or negligent vulnerabilities in their products would provide greater certainty and a strong incentive for them to improve consumer IoT security. However, it may also provide a significant deterrent to innovation: if every new line of code risks the possibility of a lawsuit, fewer lines of code will be written.[69]

There may also be significant challenges in determining liability. A claimant generally has to establish causation, demonstrate the harm could have been foreseen and show that the manufacturer or service provider was negligent.[70] Yet establishing causation in the case of cyber-attacks is likely to be challenging, particularly when large numbers of devices are involved, and the device manufacturer and the source (and victims) of the attack may be spread over multiple jurisdictions. If an unpatched device is one of thousands involved in a DDoS attack on a victim in another jurisdiction, to what extent does its manufacturer bear liability?

A further challenge comes from the lack of available information, both on the extent of harm and on what constitutes acceptable minimum security standards.[71] This adds to the difficulty of designing a new liability regime. In addition, general liability law may not cover services (for example, Directive 85/374/EEC in the European Union covers products only). This raises additional considerations – for example, do software updates to consumer IoT count as a service, or they integral to the device?

Many companies would seek to insulate themselves from lawsuits and penalties through insurance. The benefit of that would be that risk management companies and insurers would have clear motivations to establish standards, testing and criteria for the security in IoT devices. Thus, the relationship between liability laws, consumers and producers may mean that insurers step in as a neutral, third-party agent of change for security in consumer IoT.

3.11 Summary

Figure 3.2: Summary of pros and cons of each mechanism

Mechanism	Advantages	Disadvantages
Consumer education	• Relatively low cost to implement • Helps resolve information asymmetry problem	• Hard to engage consumers on the topic • Difficult to convey technical information to a largely non-technical audience • Vulnerable devices will still be available for purchase
Product reviews and comparisons	• Relatively low cost to implement • Helps resolve information asymmetry problem	• It may be difficult for non-technical reviewers to accurately assess device security • Vulnerable devices will still be available for purchase

[67] Bundesnetzagentur removes children's doll "Cayla" from the market - https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/17022017_cayla.html?nn=404422
[68] ANEC and BUEC (2018), *"Cybersecurity for connected products – a position paper"*, https://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf
[69] Moore (2010).
[70] Éireann Leverett, Richard Clayton and Ross Anderson (2017), *"Standardisation and Certification of the Internet of Things"*, WEIS 2017
[71] *Ibid.*

© 2019 Plum Consulting

Mechanism	Advantages	Disadvantages
Self-certification/ voluntary codes of practice	• Relatively low cost to implement • Encourages improved device security • May allow greater flexibility (compared to mandatory certification schemes)	• Manufacturers may not join the scheme • A self-regulated standard may only result in marginal improvements in security • Vulnerable devices will still be available for purchase
Vulnerability disclosure and vulnerability markets	• Allows vulnerabilities to be identified and patched	• Manufacturers may not fix vulnerabilities in a timely manner (or at all) • May increase the number of identified and publicised vulnerabilities
Consumer product labelling and trust marks	• Consumers familiar with product labelling schemes • Helps resolve information asymmetry problem	• Difficult to convey technical information on the label or via trust mark • Labels may quickly become outdated as new vulnerabilities discovered • Vulnerable devices will still be available for purchase
Government initiatives	• Provides incentives for better device security • Helps correct for negative externalities of insecure devices	• Difficult to set required security standards and/or rebates and subsidies at the appropriate level (and so may distort the market) • May be prone to 'gaming' by manufacturers and vendors • Requirements would need to be regularly updated to keep up with the market • Potentially costly to implement
Mandated security requirements	• Provides for a minimum level of security in the IoT device market • Helps correct for negative externalities of insecure devices	• Hard to set requirements at an economically efficient level • The market must be monitored on an ongoing basis to enforce the regime • Requirements would need to be regularly updated to keep up with the market
Mandated certification	• Reinforces a regime of mandated security standards • Raises consumer awareness	• Testing and certification may add to device costs • May be prone to 'gaming' by manufacturers and vendors
Liability reform	• Resolves problem of misaligned incentives in the market	• Difficult to implement in practice – requires significant regulatory and legislative change • Significant deterrent to innovation in the market

3.12 No intervention

When appraising the options for intervening in a market, it is considered good practice to also appraise the consequences of taking no action.

Broadly speaking, there are two major offsetting trends in IoT security:

- Firstly, the rapidly growing number of devices. The installed base of consumer IoT devices is expected to grow to around 13bn devices by 2020, from 7bn today.[72] This increase represents additional risk: not

[72] See Figure 1.1.

© 2019 Plum Consulting

only will there be more devices out there to be compromised, but botnets will also grow in scale and power.

- Secondly, market developments towards improved security. Growing consumer awareness of cybersecurity, new IoT-related standards and services, improvements in ISPs' network protection measures and the increasing penetration of big-name brands in the market all signal a trend towards better security on devices and networks.

At this stage, it is difficult to say whether the net effect of these trends is to improve or worsen IoT device security. It has been argued that, despite a bleak picture painted by the headline trends, online security is actually improving year on year.[73] Yet the consumer IoT market is growing rapidly, and consumer IoT devices are now disproportionately involved in cyberattacks.[74] Such devices have provided a massive resource for botnet operators, meaning they can now launch attacks of over 600 gigabits per second – enough to overwhelm almost any website or network resource. By targeting financial services or utility networks, botnets made up of huge numbers compromised IoT devices have the potential to cause widespread disruption.

It appears unlikely that market-driven security improvements will spread widely and quickly enough to offset the rapid growth in consumer IoT devices, at least in the short-term.[75] This suggests there is some role for measures that aim to improve the security on such devices and services. However, the application of these measures must be considered and proportionate so as not to deter market development and innovation: in the long term, market trends, including consumer awareness, product differentiation, and mobile network operator market entry, can be expected to improve device security. The effectiveness and side-effects of these measures should also be assessed at regular intervals.

It should also be noted that there is an existing installed base of devices that will not be affected by remedial measures aimed at new devices. This means that the issues created by poor security on consumer IoT devices (such as botnets) are likely to persist over the near-term. However, this will diminish over time as older devices are replaced by new devices with better security measures.

[73] Eric Jardine (2017), *"Sometimes Three Rights Really Do Make a Wrong: Measuring Cybersecurity and Simpson's Paradox"*, Paper presented to the 16th Annual Workshop on the Economics of Information Security

[74] See for example https://www.akamai.com/us/en/multimedia/documents/social/q4-state-of-the-internet-security-spotlight-iot-rise-of-300-gbp-ddos-attacks.pdf and https://krebsonsecurity.com/2018/05/study-attack-on-krebsonsecurity-cost-iot-device-owners-323k/

[75] See Section 2 for analysis of growth trends in the consumer IoT market.

© 2019 Plum Consulting

4 Potential actions to improve the security of consumer IoT devices

This section discusses potential actions to help address the market failure in the consumer IoT market. These actions represent practical implementations of the measures discussed in Section 3 and have been developed to address (or mitigate) the economic factors discussed in Section 2: information asymmetry, misaligned incentives; and negative externalities. They also take into account the ongoing development of the market, with the goal of fostering future innovation and development and still achieving improvements in device security.

To be effective, any solutions are likely to require engagement from policymakers and industry. In addition, these solutions will have to strike a balance between improving security and allowing scope for innovation and evolution within the market.

Below we suggest a number of potential actions to address the economic factors. These actions are intended to improve the security of consumer IoT devices and services on the market, and to encourage manufacturers to adopt a 'security-by-design' philosophy, where security is considered at all stages of product development, sale and ongoing support.

This set of potential actions has been developed after consideration of a wider number of mechanisms, and the pros and cons of each mechanism, for improving security on consumer IoT devices and services. A number of mechanisms were selected on the basis that the potential benefits (in terms of improved device security) were likely to outweigh the costs of implementation.

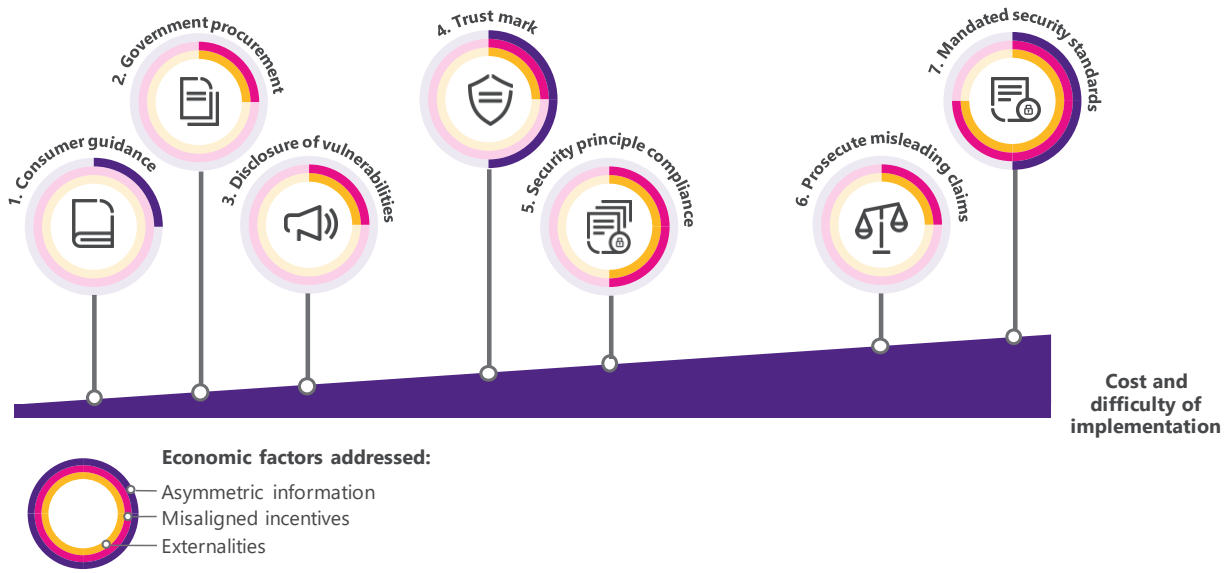
From these mechanisms we developed a set of specific, tailored actions for the industry and policymakers to take. These actions are illustrated in Figure 4.1. They are listed in order of the likely cost and difficulty of implementing the action. Figure 4.1 also denotes the efficacy of each action in alleviating (or compensating for) each of the three economic factors behind poor security on consumer IoT: asymmetric information, misaligned incentives and externalities.

The actions are aimed at a variety of stakeholders in the market: actions by different stakeholders are likely to complement each other in addressing the various economic factors behind poor security. As such, the actions are not mutually exclusive; instead they are likely to reinforce each other and help to deliver better outcomes for society Security measures in the actions are taken to refer to security against both inward and outward threats, in order to protect both the user, third parties and the Internet.

It is important to acknowledge that the risk from insecure consumer IoT devices is a global problem: while one country may take steps to keep insecure IoT devices off its domestic market, it will still face risks from insecure devices in other jurisdictions. Growth in connected devices across the world will likely lead to increased transnational liability, security and privacy issues, which existing legal cooperation frameworks may be ill-equipped to handle. Cross-national, regional and global multi-stakeholder efforts to enhance consumer IoT security should be encouraged where possible.

© 2019 Plum Consulting

Figure 4.1: Potential actions and their efficacy against the economic factors behind poor IoT security



The potential actions are discussed in greater detail below.

1. **Industry bodies and policymakers should prioritise raising awareness of consumer IoT security issues, and provide guidance to buyers.** Providing information to consumers on the possible impacts of insecure devices and the need for them to seek out secure devices and services will empower consumers to make better buying decisions and help correct information asymmetry in the market. For example, in the UK, the Information Commissioner's Office provides such guidance for consumers considering buying IoT products.[76]

2. **Governments should specify a set of security outcomes for their own procurement procedures.** Governments can and should leverage their role as major purchasers to incentivise manufacturers to improve their product. These improvements in security may spill over into the consumer market – it may be easier or cheaper for manufacturers to include the same (improved) security measures in all their products, including consumer products.. The development and documenting of minimum security outcomes could also be the first step in developing a trust mark.

3. **Industry and policymakers should encourage responsible disclosure of software vulnerabilities in consumer IoT.** Policymakers could act to reduce the legal risks faced by security researchers looking to responsibly disclose information on software vulnerabilities they have discovered. Currently such researchers can face legal threats for their actions. Policymakers could create a process for responsible disclosure that reduces the risk that legitimate security researchers will be exposed to legal threats.

4. **The industry should develop a trust mark for secure consumer IoT devices.** A trust mark will facilitate consumers' ability to distinguish between devices at point of purchase, and neatly embodies detailed information. It is also a complement to the awareness raising of publicity about cybersecurity issues. It will assist in resolving information asymmetries in the market, incentivise companies to improve security, and establish an industry process to agree security standards. The trust mark might be based on an existing certification scheme or industry initiative.[77]

[76] Steve Wood (2017), *"The 12 ways that Christmas shoppers can keep children and data safe when buying smart toys and devices"*, Access at: https://ico.org.uk/about-the-ico/news-and-events/blog-the-12-ways-that-christmas-shoppers-can-keep-children-and-data-safe-when-buying-smart-toys-and-devices/

[77] An example of this is the Internet Society's Online Trust Alliance (OTA) IoT Trust Framework.

© 2019 Plum Consulting

5. **Policymakers should require that consumer IoT devices must comply with a set of security principles.** Rather than a rigidly-specified set of prescribed standards, this would involve compliance with various generalised principles – for example, requiring that:

   - the software/firmware on a device can be updated if necessary;
   - the device does not ship with easily-guessable default credentials, or credentials that cannot be changed by the user; and
   - the manufacturer complies with vulnerability disclosure standards.

   This approach should lead to improved device security while retaining flexibility for the market to innovate and improve on security measures.[78] The principles are more likely to remain future-proof (whereas specific encryption methods may eventually become obsolete) and will also apply to new classes of devices.

6. **Policymakers should be more proactive in prosecuting manufacturers or service providers who make misleading claims on security.** This measure would provide an incentive to manufacturers to either improve security or provide honest information about the security on their devices. It could also tie into a wider education/publicity campaign. The US has been active in pursuing device manufacturers that mislead consumers about the level of security on their devices.[79][80]

7. **If the above actions do not result in material improvements in consumer IoT security, regulators could mandate a minimum set of security requirements for IoT devices.** The actions listed above are aimed at improving consumer IoT security without the need for extensive government intervention. However, if industry-led initiatives fail to lead to material improvements in device security, policymakers should be prepared to consider mandating a set of security requirements for consumer IoT, with or without certification.

   This represents a logical extension of Action 5. The main distinction is that, under this approach, the security requirements of a product are much more tightly specified at a technical level – for example, specifying a minimum strength of encryption, or certain criteria for the default credentials (e.g. length). This action could be further reinforced by more rigorous testing of products entering the marketplace to ensure compliance.

   Minimum security requirements may reduce the risk of a device being compromised, and the resultant costs. However, they may also add to the cost of producing and maintaining devices, which could increase prices and reduce adoption (thus decreasing the benefits of connected device adoption for users and wider society) and/or encourage a "black market" in non-compliant devices.

   It is possible that, for some specifications of the minimum security requirement, the costs (in terms of foregone benefits) will outweigh the benefits. It may be difficult to accurately assess these costs and benefits. As a result, it is recommended that this approach is employed only if other measures prove ineffectual.

https://www.internetsociety.org/iot/trust-framework/

[78] In the UK the Department for Culture, Media and Sports (DCMS) offers "Security by Design" recommendations to industry (see https://www.gov.uk/government/publications/secure-by-design). These formed the basis for an ETSI industry standard (see https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf).

[79] In 2017 the Federal Trade Commission (FTC) fined Vizio, a smart TV manufacturer, $2.2m after it was found to be monitoring the operation of its devices without consent https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it

[80] The FTC also filed a complaint that device manufacturer D-Link left its devices vulnerable to hackers, contrary to claims made by D-Link.[80] Though the complaint was dismissed by the court, such actions send a signal to manufacturers that there is the *potential* to be found liable for consumer harm if they mislead consumers on security, helping to address misaligned incentives in the marketplace. https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate

© 2019 Plum Consulting

Appendix A Consumer IoT market

To help understand the vast array of technical, social and economic issues raised by the IoT, the overall market is often divided into verticals – markets where vendors offer IoT devices, services and data analytics to a specific industry or group of customers with a particular set of needs.

This study focuses on the consumer IoT market. This market can be further divided into three broad subcategories:

- Home and residential, comprising smart TVs, smart appliances, voice-activated home assistants, intelligent utility devices, wireless printers and scanners, home automation tools, baby monitors, cameras and other home security products.
- Transportation, including both in-vehicle and external systems linked to personal transport.
- Health, fitness and personal, including personal safety alarms, healthcare devices, and wearable devices (e.g. Fitbit, Apple Watch, etc.).

A.1 Size of the consumer IoT market

A famous and oft-quoted estimate of the scale of IoT is Cisco's 2011 prediction that there would be 50 billion IoT devices connected by 2020 (though this estimate was subsequently revised downward).[81] Gartner has estimated that there were 8.4 billion devices in use in 2017, and predicted there would be over 20 billion devices by 2020.[82] IHS Markit, meanwhile, has estimated that there were nearly 27 billion IoT devices in use worldwide in 2017, and forecasts this will jump to 125 billion by 2030 (this forecast includes smartphones and tablets).[83]

It is clear that early estimates of the growth of the consumer IoT market were overly optimistic. However, it is also clear that – despite the considerable disparity between the various forecasts – IoT is both large and growing quickly.

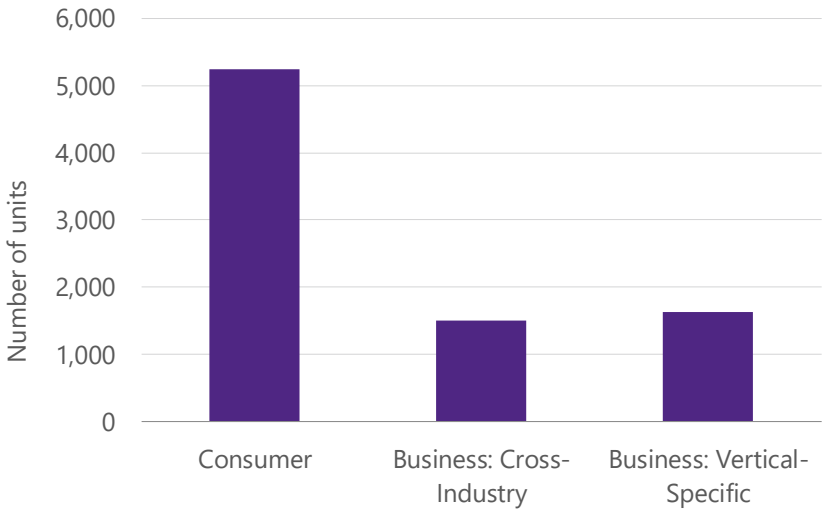
Many industry analysts also include smartphones as part of the consumer IoT marketplace. However, this skews the analysis of the market and it significantly changes the way that security risks and vulnerabilities are addressed. The smartphone is an important part of the consumer IoT landscape because it acts as hub for connectivity: many services that consumer IoT devices provide are integrated with apps and services running on a phone. However, a recent study shows that smartphone use would dominate and obfuscate any analysis of the consumer IoT market.[84] For the purpose of this report, the consumer IoT market is presumed to exclude smartphones.

Consumer IoT devices comprise the largest share of the total IoT market. According to Gartner, consumer devices (excluding smartphones and tablets) comprised 63% of the total installed base of IoT devices in 2017 (Figure A.1).

[81] https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated
[82] https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016
[83] https://technology.ihs.com/596542/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030-ihs-markit-says
[84] For instance, in answering the question "Which of the following Internet-connected devices have you used in the last 12 months?" smartphones are mentioned twice as many times as any other IoT device. See Economist Intelligence Unit (2018), *"What the Internet of Things Means for consumer privacy?"*, https://www.forgerock.com/resources/view/68775648/analyst-report/what-iot-means-for-consumer-privacy.pdf [EIU (2018)]

© 2019 Plum Consulting

Figure A.1: Installed base of IoT devices by category (2017)



Source: Gartner[85]

The consumer IoT market is also growing more rapidly (Figure 1.1).

A.2 Types of consumer IoT device

What kinds of device are fuelling the rapid growth of the consumer IoT market? The largest segment of the market is Home and Residential IoT devices: the dominant consumer IoT device, worldwide, is the smart TV. Between 25-35% cent of consumers worldwide own a television that can connect to the Internet.[86]

Beyond smart TVs, the remainder of the Home and Residential IoT category is still nascent, but growing rapidly. Smart speakers and voice assistants are the next most widely-deployed home IoT devices. Neither Google nor Amazon publish sales numbers, but, Alpine.AI, the developer of the voice recognition software for these devices, predicted that there would be 33 million voice-first devices in circulation in 2017[87] (for comparison purposes, in the same period, it was expected that there would be 450 million smart TVs in consumers' homes).

Home automation devices, including security devices (such as the connected door lock), smart lighting and smart thermostats, are also growing quickly. Other notable residential IoT devices include smart appliances, garden equipment and toys. As well as recognised brands such as Nest, there is a wide variety of companies active in this segment, many of whom are not originally technology companies. For example, connected lightning products are being sold by Philips, Osram and GE. Many of these devices are relatively inexpensive.

Figure A.2 provides an estimate of the value of sales, and corresponding growth, for some of the most popular types of smart home device.

[85] The cross-industry business category represents devices like smart security systems, which have wide applicability. The vertical-specific category includes devices such as connected manufacturing equipment and sensors for use in power plants.
[86] Deloitte (2017), *"Global Mobile Consumer Trends"*, https://www2.deloitte.com/ng/en/pages/technology-media-and-telecommunications/articles/global-mobile-consumer-survey.html
[87] Alpine.AI (2017), *"The Voice Report"*, https://alpine.ai/the-2017-voice-report-by-alpine/

© 2019 Plum Consulting

Figure A.2: Sales revenue by category of smart home device

Product category	2017 (US$M)	2022 forecast (US$M)	Forecast CAGR, 2017-2022
Video entertainment	$133,091.48	$201,063.36	9%
Smart Voice Assistants	$4,401.39	$17,431.00	32%
Home Monitoring/Security	$4,271.30	$12,136.50	23%
Lighting	$1,120.53	$3,511.32	26%
Thermostat	$1,774.35	$3,875.91	17%
Others	$17,532.54	$38,963.93	17%
Total	$162,191.59	$276,982.02	11%

Source: IDC Worldwide Quarterly Smart Home Device Tracker, March 2018

Globally, the category of Transportation IoT is significantly smaller than Home and Residential IoT: between 2% and 4% of those surveyed said that they own or have access to a connected vehicle. The notable exceptions are China and India, where the proportion increases to 18 and 15% respectively. However, it is easy to project that this will change as eCall[88], the European initiative to bring rapid assistance to motorists in an urgent situation anywhere in the European Union, comes into effect from 2019 for new automobile sales.

The health and personal IoT category is dominated by wearables: fitness trackers and smart watches. 15% of the world's population currently have a wearable device, with numbers closer to 20% for Russia and China.[89] The trend within this category is toward smart watches and away from fitness trackers: smartwatch sales went up by 60% in 2017,[90] while sales of fitness trackers fell by 18% in the same year – to 40 million units, 23% lower than its peak in 2016.

The wearables market tends to be dominated by larger companies: just two companies account for 80% of the fitness tracker market.[91] Apple is the largest player in the smartwatch market, shipping 16m smartwatches in 2017 and emerging as the overall leader in the wearables category.[92]

However, a telling trend in the health and personal IoT category is that long-term use and satisfaction is proving difficult for companies making fitness trackers. These companies, like Fitbit and Xiaomi, see high sales over holiday periods, but then fail to retain users. In one survey, a quarter of new users claimed that wearables had failed to meet their expectations, citing limited functionality and connectivity as major complaints.

A.2.1 Marketplace dynamics

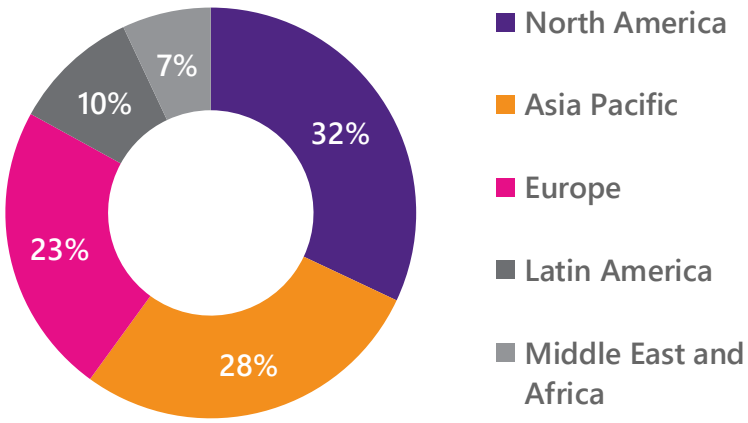
Regional dynamics

North America and the Asia Pacific dominate consumer IoT in terms of size, collectively comprising around 60% of the global market by revenue. Europe is the next largest, with 23% of the global market. Latin America and Africa and the Middle East comprise 10% and 7% of the global market respectively.

[88] European Parliament, Regulation (EU) 2015/758, 5 May 2015.
[89] Deloitte (2017), *"Global Mobile Consumer Trends"*, https://www2.deloitte.com/ng/en/pages/technology-media-and-telecommunications/articles/global-mobile-consumer-survey.html
[90] https://www.engadget.com/2017/08/31/smartwatch-market-performing-well/?guccounter=1
[91] Fitbit and Xiaomi.
[92] https://www.idc.com/getdoc.jsp?containerId=prUS43598218

© 2019 Plum Consulting

Figure A.3: Regional IoT revenue split



Source MarketResearch

The regional market shares reflect the availability of supporting Internet infrastructure in each region (a connected device is only useful when Internet connectivity is available and reliable). They also reflect the relative affordability of the technology in those regions, with richer regions purchasing more IoT devices and services.

Component Dynamics

Among the three major components of consumer IoT systems – hardware, software, and services – the hardware segment is expected to contribute the major revenue share in the global IoT market. The hardware segment's share in terms of revenue to the global market is expected to be 37% in 2021. Internet-enabled hardware, edge devices and chips such as processors and sensors are examples of hardware used in the IoT market.

Examples of the software in the global IoT market are embedded software, hub software, communication software, security solutions, data management software, and so on. Software's share of the market is estimated to be about 35%.

Supplier Dynamics

There are a huge number of companies in the marketplace in all three major components of consumer IoT systems (hardware, software, and services). Some companies, such as Google or Amazon, attempt to compete globally with products in all three major component areas. Other companies, such as Xiaomi, are competing in a single market and attempting to customize products based on the needs and desires of regional customers.

An important trend in the software and services side of consumer IoT is the development of proprietary frameworks – hubs or gateways around which third party solutions can be built. The classic example of this in consumer IoT is Amazon's voice assistant device, Alexa. The barrier to entry to compete with Google Home, Microsoft Cortana and Amazon's Alexa is extremely high, but the ability to build services around those platforms is made easy through publicly available application platforms. In the case of Amazon's Alexa, third parties are invited to develop "skills" for Alexa. Third-party applications using an existing consumer IoT platform represent a major trend in the software and services components of consumer IoT.

However, one of the biggest challenges consumer IoT is facing is the lack of cooperation within the industry to create a unified IoT framework. A unified framework would provide a set of standards where different vendors' services and applications could interoperate. The goal would include an open platform where one vendor's hardware could be used by other vendor's applications or software, rather than vendors creating solutions

© 2019 Plum Consulting

independently. To a limited extent this has occurred in the "smart speaker" ecosystem, where vendors work to make their products compatible with familiar, voice-based commands offered by one or two providers. However, this is a reflection of market dominance by certain vendors, rather than an attempt to provide an open standards-based, interoperable IoT technical framework.

In hardware, companies have begun to offer multi-purpose hardware platforms for the development of consumer IoT solutions[93]. Typically, a third party building a new consumer IoT device will use this platform as a building block for prototyping. If successful, the prototyped device will emerge from its "general purpose" origins and be built and customized for its specific application.[94]

Similar companies have emerged in the services space to allow IoT developers to use Software as a Service to avoid the cost of setting up the services themselves. An example of this is Jasper, which focuses on cellular connectivity.[95] Microsoft is leveraging its Azure platform to offer an IoT 'hub' to connect and manage IoT devices.[96] Mobile network operators increasingly view the consumer IoT segment as a market opportunity, allowing them to leverage capabilities of SIM-based secure network access with their experience in industrial IoT applications including apps, security, location and monitoring.[97]

The Impact of Data

While not a component of the hardware sold to consumers, it is important not to underestimate the impact of data collection from consumers. For some vendors, the collection, processing and marketing of anonymised or pseudonymised consumer data is a crucial – and sometimes essential – part of the revenue stream for IoT device manufacturers. In some cases, the device itself is sold with minimum mark-up in anticipation of the value of the revenue/value/profit from consumer data. While not strictly a component of what is sold to the consumer, it makes up an important part of the revenue generated for the manufacturer.

[93] As an example, in February 2018 Mozilla introduced its "Project Things." It has the goal of building a decentralized 'Internet of Things' that is focused on security, privacy, and interoperability. In February the organization took a first step by making it possible to use a Raspberry Pi to build a "Things Gateway." Besides being controlled from the web, the Things Gateway is also capable of responding to voice commands and controls.
[94] As an example, see https://www.particle.io/
[95] As an example, see http://www.jasper.com/
[96] See https://azure.microsoft.com/en-us/services/iot-hub/
[97] https://www.digitaltveurope.com/2018/07/06/vodafone-portugal-kicks-off-with-consumer-iot-services/

© 2019 Plum Consulting

Appendix B Developments in IoT security

B.1 Financial investment in IoT security

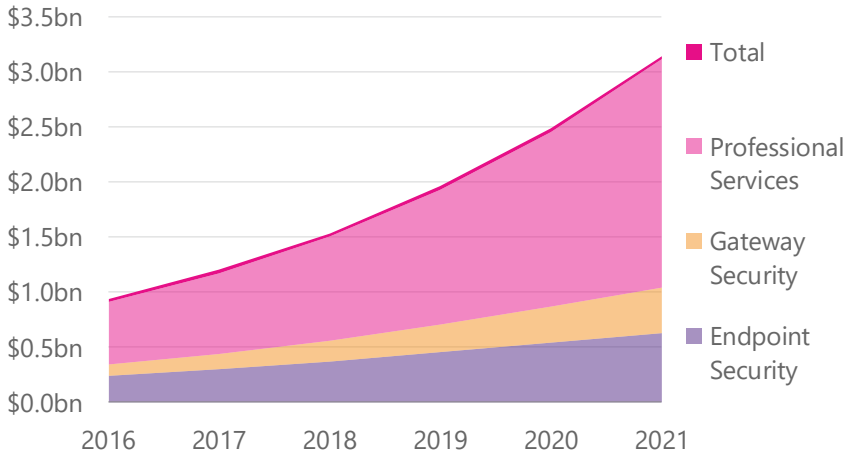
In the development of consumer IoT devices, manufacturers and developers have a finite set of resources at their disposal. In the end, a large amount of those resources is used to build supporting Apps, attractive systems and services, with security as more of an afterthought.

In the recent past, new companies have moved into the consumer IoT device space, often operating with tight margins that are typical for hardware and application product development. Adding sunk costs like software development and security provision makes achieving a return on investment harder. Whirlpool has estimated that adding intelligence to a dishwasher would add about $5 to the cost of the product; while this may not be substantial compared to the overall cost of a dishwasher, the cost is largely fixed and could be highly significant for lower cost, lower-margin devices. Adding security features may also make it harder for developers to build "families" of complementary consumer products.

This environment is different from traditional computers or smartphones. In those cases, large companies spend significant resources on testing code before it is released to consumers. When vulnerabilities are found, the underlying software is often patched. This isn't the case with consumer IoT systems like home thermostats or appliances: those electronics are made and sold at a much lower margin, and the companies involved often don't have the resources – or the expertise – to make them secure.

Nevertheless, there is some evidence to show that investment into IoT security has been growing. Gartner forecasts that spending on IoT security will double by 2021, though the bulk of this increase is attributable to professional services. It is also not clear how much of this expenditure will be directed at consumer IoT devices.

Figure B.1: IoT security spending worldwide



Source: Gartner

Direct measures of corporate financial investment in IoT security is difficult to obtain. However, Juniper Research estimates that 5% of global, total cybersecurity spend is dedicated to IoT (including both consumer and industrial segments).

While the vast number of investments in IoT are investments in platforms, some evidence of the commercial importance of IoT security comes from investors. IoT security firm Armis has raised $46 million in venture capital

© 2019 Plum Consulting

funding for its products and services. In September 2017, San Francisco-based Bastile raised $27 million for threat detection applications. In May this year, LockState raised $5.8 million in investments.

B.2 Consumer attitudes to security

A survey of over 10,000 consumers in 2017[98] found that 90% of consumers were "concerned about IoT security." More than half of those listed four key threats as part of their concern:

- weaknesses that lead to outside entities having control of consumer devices (65%);
- consumer IoT products leaking sensitive data (50%);
- unauthorized external entities having access to information via IoT devices (54%); and
- attackers using consumer IoT devices as a platform to conduct other attacks (50%).

This finding is echoed by a variety of other surveys. A 2018 survey of over 1,600 consumers found that 90% were concerned about the possibility of identity theft or fraud from the use of connected devices.[99] A 2017 study by Consumers International noted that 60% of people worldwide report concerns about connected objects, and 43% of people didn't trust the IoT sector.[100]

Similarly, in a survey of 3,000 consumers conducted by Cisco in 2017, only 9% of consumers had a high level of trust that their data collected and shared via IoT is secure. Yet in spite of that extremely low level of trust, a very large number of consumers – 42% - indicated that they were unwilling to disconnect their IoT devices because of the value those devices and services provided. 53% of respondents said that the technology made their life easier.[101]

This reflects a fundamental paradox in consumer IoT security: consumers indicate widespread concern over the security and privacy of connected devices, yet continue to purchase connected devices in large (and growing) numbers

Moreover, once devices are purchased, relatively few consumers take basic security precautions: fewer than 40% of consumers who own an IoT device ever change the default password on their IoT devices. A 2017 survey indicated that only 31% of consumers that own connected devices perform updates as soon as they become available (a further 40% of consumers have never updated their devices).[102] Even among the group of consumers that describe themselves as "intermediate or advanced" with regard to technical literacy, nearly 70% don't change the passwords on their connected devices from the factory default passwords.

B.3 Market developments in IoT security

Significant growth in industrial IoT, standards development and volume manufacturing are all likely to impact the security of consumer IoT devices and services. In addition, market trends in consumer IoT are also likely to lead to enhanced device security.

[98] Gemalto (2017), *"The State of IoT Security"*, http://www2.gemalto.com/IoT/#accessa11
[99] EIU (2018)
[100] Consumers International (2017), *"Testing our trust: Consumers and the Internet of Things – 2017 Review"*
[101] Cisco (2017), *"The IoT Value/Trust Paradox - Building Trust and Value in the Data Exchange Between People, Things and Providers"*, https://www.jasper.com/resources/reports/iot-value-and-trust-survey?ecid=af_700000005
[102] Canonical for Ubuntu (2017), *"Taking charge of the IoT's security vulnerabilities"*, https://pages.ubuntu.com/IoT-Security-whitepaper.html [Canonical for Ubuntu (2017)]

© 2019 Plum Consulting

Some prominent developments include:

- Standards development in mobile networks, including support in new ETSI Releases for high density, wide area coverage networks to support IoT applications. This is intended to be implemented by Mobile Network Operators (MNOs) to support new connected devices and services (e.g. camera, location trackers and monitoring)[103] across multiple mobile frequency bands. These devices are devices likely to be more secure than their Wi-Fi counterparts.

- The development of the WPA3 (Wi-Fi Protected Access) standard. WPA3 will begin to be available in 2019 and will add new features to devices and home routers to simplify Wi-Fi security and to enable more robust authentication and increased cryptographic strength. WPA3 will be backwards-compatible with existing WPA2 access networks.

- Market entry by brand name consumer product providers such as Nest, Google Home, Apple and Amazon, and MNO-branded home monitoring and location tracking-type applications. Unlike white label manufacturers, established brands are more likely to be concerned with the possibility of reputational damage as a result of poor security on their devices. As a result, they have a greater incentive to include effective security measures.

- Improvements in ISP network security practices, including DDoS identification and remediation and related network-level defences against attacks.

[103] See https://www.digitaltveurope.com/2018/07/06/vodafone-portugal-kicks-off-with-consumer-iot-services/

© 2019 Plum Consulting

Appendix C Categories of consumer IoT threats

C.1 Threats to the device owner's safety

Consumer IoT devices are not evaluated in the same way as other home devices that have the potential to create life-threatening situations in the event they fail, such as electrical circuit breakers, electrical cords and transformers. There are also physical safety hazards of devices as simple as Wi-Fi-enabled lightbulbs and appliances. The risk is that consumer IoT devices potentially introduce physical safety threats as well as security threats.

Those threats might include:

- IoT-enabled smart meters & thermostats – remote access to these could give an intruder the ability to alter temperature in a building to extremely low or high values that could, as an example, affect the health of elderly or unwell occupants, or in extreme cases start a fire or gas leak
- IoT-enabled home sensors – disabling sensors such as smoke detectors and carbon monoxide alarms risks harm to a building's occupants.
- IoT-enabled lightbulbs – remote access to these devices might allow for remote control of the on/off switch – or, brightness - which could affect the personal safety of residents suffering from poor eyesight or sensitivity to very bright or very low levels of ambient light
- IoT-enabled washing machine – the ability to remotely overload the spin or door control of these devices could cause flooding and/or physical eruption of the machine, which could be extremely dangerous to consumers in its vicinity
- IoT-enabled ranges or ovens – the ability to remotely tamper with oven controls might result in a dangerous gas leak or the establishment of temperatures that were dangerously high
- IoT-enabled door and garage locks – the ability to tamper with IoT door locks could affect the safety and security of occupants or might be used to deliberately lock them in their own homes/rooms for illegal purposes.
- IoT-enabled teapots & coffee machines – the ability to turn these devices on remotely, potentially when they don't have water in them, might result in the heating element becoming too hot with the potential to start a fire

Almost all of these potential safety threats have been demonstrated in lab and research conditions, as well as in demonstrations at security events. While seemingly harmless additions to the convenience of a consumer's home life, these devices also put unsuspecting consumers at potential physical risk in their home.

C.2 Threats to owner privacy

The challenge to personal privacy is significant in the context of consumer IoT devices. As more and more devices collect data, share it and monetize it, the IoT environment monetizes personal information at the device level. It is already clear how this works at the smartphone level, where many apps already collecting data at the user's expense and then selling it in ways that are not obvious or explicit to the consumer. In the IoT environment, not one, but many devices may interact in complex and unexpected ways. In the absence of new

© 2019 Plum Consulting

and explicit mechanisms for explaining what data is being collected – and how it will be used – consumers will be unable to understand the privacy implications of their own choices.

In some settings, such as health care, there are clear regulations that determine what is legal data collection and use. However, wearables are often not considered to be medical devices subject to the protections afforded to healthcare data.

The result is that consumer IoT devices can potentially represent a threat to consumer privacy, for example:

- Terms of Use - Many IoT consumer devices require initial registration of an account by the end-user, and acceptance of some sort of End User License Agreement (EULA). Often these EULAs are long and in small print and not read by the consumer before acceptance, yet in many cases they set out the possible personal nature of data that their devices and systems intend to collect, process and store. In addition, many EULAs indemnify the manufacturer and application developers against any attempts to claw back rights related to privacy and use of personal data. However, the consumer is only left with a binary choice – accept the terms or don't use the product or service.

- Voice-based Personal Assistants – This class of consumer IoT device is particularly popular but its ability to have a consumer interact with a variety of services using voice is also the source of privacy risks. The result is that these devices can listen for, collect and share information with the consumer's knowledge and consent.

- Health monitoring & tracking devices – Many IoT health tracking devices record health data and GPS location if used as part of exercise regimes, e.g. fitness trackers. Any exposure of an individual's GPS location could have privacy implications for that individual. As a result, many military organizations are prohibiting the use of consumer-grade personal fitness and tracking devices

- Smart TVs and toys which record speech for some sort of control or interaction with the consumer IoT "smart" device – In addition to voice-based personal assistants, internet-connected TVs have been found to violate consumer privacy rights by recording private conversations without consent. Similarly, some children's toy manufacturers might also be in breach of privacy laws due to their recording, processing and possible storage of children's.

C.3 Threats to availability

The tension between ease of use, functionality and security is nowhere more apparent than in the area of availability. As consumers come to depend on these devices for important or necessary parts of their daily life, the IoT devices' threats to the availability of critical personal resources becomes extremely important. Examples of consumer IoT threats to availability might include:

- Eliminating access to fresh water – where IoT devices helping control and monitor the usage of consumer water supply, it is potentially possible to remove access to water by using an IoT device to close access to the source of the water.

- Removing access to electrical power – IoT devices are a part of every installation of consumer solar cells. By interfering with the controls for the redistribution of residential power into the traditional power grid, an electric utility would be forced to remove the connection of the resident to the power grid. The result would be the elimination of power supply for a consumer because of the weakness of security in the devices supporting the alternative power source.

© 2019 Plum Consulting

- Removal of access to emergency services – Many seniors are now depending on voice activated personal assistants as a source of personal safety. The ability to simply use one's voice and make a call for help is a functional improvement over having to find and push a button. However, voice-based assistants can have their connection to manufacturer's back-ends disrupted. In an application that provided personal safety, this would result in the removal of access to emergency services.

© 2019 Plum Consulting

Appendix D Case studies of consumer IoT threats

This appendix contains examples of security threats to consumer IoT devices, or security threats which use such devices as the basis for other types of attack.

Mirai

Perhaps the most famous example of a large-scale attack using IoT devices is the Mirai botnet, which (at its peak) comprised over 600,000 IoT devices infected by the Mirai malware. This botnet was used to perform an enormous DDoS attack on the website of security writer Brian Krebs in late 2016, taking Krebs' site offline for several days and causing an estimated US$324k in costs to the device owners alone.[104]

A later attack on domain name server (DNS) provider Dyn knocked dozens of sites offline for a day – including Amazon, Spotify, and Twitter. Dyn reportedly lost 8% of its customer base in the wake of the attack.[105]

These attacks used just a fraction of the overall power of the botnet – just 24,000 devices were used in the attack on Krebs' website. Versions of Mirai were later created that exploited particular weaknesses in specific manufacturers' devices.[106]

Smart Lighting Attacks

In 2016, researchers in Europe demonstrated a new type of attack using so-called Smart Lighting. In the first example of the attack, the researchers used smart lights as a covert light-based communication system to exfiltrate data from a highly secure (or even fully airgapped) office building. They were able to implement the attack and were able to read the leaked data from a distance of over 100 meters using only cheap and readily available equipment.

In the same paper, the researchers showed that an attacker can strobe the lights at a frequency which may trigger seizures in people suffering from photosensitive epilepsy (in the same way that rapidly flashing video games can cause such seizures). The researchers demonstrated the attacks using both high-end and lower-end smart light systems, ranging from an expensive Philips HUE system to a cheap system manufactured by LimitlessLED.[107]

Attack on Home IoT Hub Technology

Researchers have created publicly available modules for the penetration framework Metasploit that could give attackers a way to inject code into the Belkin WeMo connected switch. This could allow them to run commands with the highest privilege on the switch. The switch's firmware is encrypted with GNU Privacy Guard (GPG) but the private key has been extracted and published on the Internet. While these vulnerabilities have since been fixed by the vendor, older, non-updated IoT devices and switches remain at risk from the published attacks.

Attack on Home Monitoring Technology

Owlet is a sensor that babies wear in a sock that monitors their heartbeat and relays that data wirelessly to a nearby hub. It is intended to be a monitor that parents can use to tell (remotely) if anything is wrong with the child. The sensor connects to a proprietary base station which then communicated with the manufacturer's

[104] Kim Fong et al (2018), *"rIoT: Quantifying Consumer Costs of Insecure Internet of Things Devices",* https://groups.ischool.berkeley.edu/riot/#download
[105] https://www.corero.com/blog/797-financial-impact-of-mirai-ddos-attack-on-dyn-revealed-in-new-data.html
[106] M. Anonakakis, et al (2017), *"Understanding the Mirai botnet,"* in 26th USENIX Security Symposium, USENIX Security 2017, Vancouver BC, Canada, 2017 pp. 1093-1110
[107] E. Rosen and A. Shamir (2016*), "Extended functionality attacks on IoT devices: The case of smart lights,"* in IEEE European Symposium on Security and Privacy, EuroS&P 2016, Saarbrucken, Germany, 2016.

© 2019 Plum Consulting

servers. The Owlet base station encrypts data that is sent to and from the manufacturer's servers, which contacts parents' phones if needed. However, the ad-hoc Wi-Fi network that provides the connection between the sensor in the sock and the base station is completely unencrypted and doesn't require any authentication to access.

Any attacker who is within range of the ad-hoc Wi-Fi network can join that network and then examine packets in flight and also inject packets destined for either the sensor or the base station. If within range, an attacker can snoop on the base station's wireless network. A single unauthenticated command over HTTP can make the Owlet base station leave a home Wi-Fi network and join one of the attacker's choosing; it can also take control of the system and monitor a stranger's baby and prevent alerts from being sent out.

Attack on Heating Systems in Winter

In November of 2016, a DDoS attack was carried out on heating distribution in two buildings in Lappeenranta, Finland. In both attacks, the DDoS attack targeted the computers that controlled heating in the buildings. The effect of the attack was to continue to force the heating systems to attempt to recover by rebooting – the repeated process had the effect of never getting the heating systems turned on at all. The attack took place at a time in Finland when the temperature was below freezing. The devices targeted were known to have vulnerabilities and the source of the attacks was compromised IoT devices both local and remote to the small Finnish town.[108]

DNS Attack on Campus

A Verizon report tells of a university where more than 5,000 discrete systems were engaged in an attack where each device did hundreds of lookups at the same time. As a result, legitimate users, students and staff were unable to get Domain Name System queries answered and the result that the Internet was painfully slow or completely inoperable. While the IoT devices were configured to be in a separate network, they were also configured to use the production network's name servers. The result was traffic to the production name servers that was so intense that legitimate queries were either extremely slow to be answered, or went completely unanswered. The IoT malware spread by attempting to force itself on other IoT devices through brute force attacks on other IoT devices using default and weak passwords. Once the password for an IoT device was discovered, it was changed to that only the malware had control of the device. [109]

Detailed Attacks on Home-based IP Cameras

Researchers in China have published detailed instructions for device scanning, device spoofing and other attacks on a specific model of IP-connected camera. While the attack is specific to a particular camera model, the description of the attack is generalized enough to be adapted to any model of camera. The attack allows an attacker to discover what cameras are available in a local network, to pretend to be a legitimate camera in the network, and finally access a poorly protected backdoor that allows an attack on the CGI script that starts a variety of Internet related services.[110]

Attack on Smart Plugs

In a paper from 2017, a set of researchers examined the state of security with some commercially available Smart Plugs. Smart plugs have been install by many consumers and often use voice-activated digital assistants or smartphones as a control vector. The authors of the paper were concerned that the smart plugs represented a security threat in themselves.

[108] Metropolitan.fi (2016), *"DDoS Attack Halts Heating in Finland Amidst Winter"*, http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter
[109] Verizon (2017), *"IoT Calamity: the Panda Monium"*, http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-sneak-peek_xg_en.pdf
[110] Zhen Ling et al (2018) "IoT Security: An End-to-End View and Case Study," *arXiv preprint arXiv:1805.05853*

© 2019 Plum Consulting

The authors discovered that some popular smart home plugs have severe security vulnerabilities which could be fixed but unfortunately are left unpatched by vendors. In the research paper, the authors take a specific, commercially available smart plug and launch four exploits based on the security frailty of the underlying system: 1) a device scanning attack; 2) brute force attack on the devices themselves; 3) spoofing attack; and 4) a firmware attack. All of the attacks were practical examples of attacking a commercially available, well-known smart plug device and showed that it was possible to obtain authentication credentials from the owners by performing these attacks.[111]

[111] Zhen Ling et al (2017), "*Security vulnerabilities of internet of things: A case study of the smart plug system.*" IEEE Internet of Things Journal 4, no. 6 (2017): 1899-1909.

© 2019 Plum Consulting

© 2019 Plum Consulting London LLP, all rights reserved.

This document has been commissioned by our client and has been compiled solely for their specific requirements and based on the information they have supplied. We accept no liability whatsoever to any party other than our commissioning client; no such third party may place any reliance on the content of this document; and any use it may make of the same is entirely at its own risk.