The economics of consumer Internet of Things security

Sam Wood, Mark McFadden

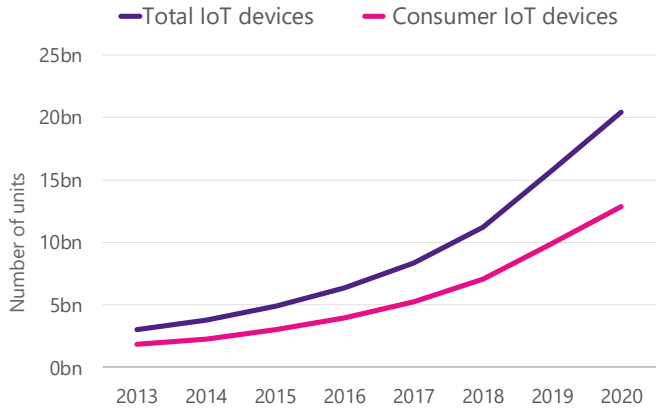
Connected consumer devices – such as smart TVs, smart thermostats and connected appliances – are becoming increasingly common. Yet the cybersecurity measures on these devices are often lacking: many such devices contain serious vulnerabilities that leave them open to attack. While there are a number of technical reasons behind weak device security, the root cause lies in economic factors. These factors include asymmetric information, misaligned incentives, externalities and behavioural biases. Drawing upon a recent report for the Internet Society, this Insight explores these economic factors and proposes actions to help address them. These actions should help improve both device security and the security of the wider Internet.

Introduction

The Internet of Things (IoT) is a vast network of physical devices capable of connecting to the Internet. 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 estimates by Gartner, the number of IoT devices (excluding smartphones) in operation in 2018 was over 10bn[i] (while there are various estimates available, they all agree that the number is very large).

Figure 1: Installed base of IoT devices



Source: Gartner

Around two-thirds of these are 'consumer IoT' devices, intended for residential or personal use. These include smart TVs, connected appliances, smart lighting, home automation devices, home security products, wearables and personal healthcare devices.

Security risks in the IoT market

The security measures on these consumer devices are often lacking. An analysis of common types of consumer devices found that 70% contained serious vulnerabilities.[ii] Another study tested twenty consumer IoT devices against four key threat dimensions: all devices tested had shortcomings in at least one of the dimensions.[iii]

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.[iv] According to some estimates, about 4,000 new vulnerable IoT devices become active each day.[v]

The exploitation of a device's vulnerabilities can cause direct threats to the device owner's safety and privacy. For example, devices with microphones or cameras can be compromised to allow home voice recordings and images to become publicly accessible.[vi] Compromised smart locks could allow intruders access to a premises without forcing entry. And vulnerable connected healthcare devices could allow hackers to change dosage settings – in 2015, researchers reported they were able to hack connected insulin pumps.[vii]

In addition to risks to the device owner, compromised devices can be used to launch attacks on a third party. Compromised devices may be recruited into a 'botnet' – a network of thousands or millions of Internet-connected devices under the control of an attacker. 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.

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. At its peak, Mirai infected over 600,000 IoT devices.[viii] A growing concern is that a similar botnet could be leveraged to attack critical national infrastructure.

What makes consumer IoT devices vulnerable?

The proximate causes of weak device security lie in number of technical factors. These include:

- **Default credentials.** Many devices ship with easily-guessable default usernames and passwords (such as "admin" and "password")
- **Poor software and network security.** Communications between the device, the user app and the wider Internet are not always encrypted. On some devices a number of network ports may be left open by default, exposing them to common attacks.
- **Limited capability of chipsets and components.** Small and cheap chipsets and memory have weak upper limits on the strength of encryption that they can support.
- **Lack of software updates.** Many manufacturers do not issue prompt or regular updates for the software on those devices. More worryingly, some devices cannot be updated at all.
- **Lack of a secure update mechanism.** 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.

Economic factors behind weak consumer IoT security

The technical factors provide a proximate explanation of why consumer IoT security is often weak, but questions remain. If the consequences of weak security are serious, why are consumer IoT devices with weak security commonplace? Why do consumers buy 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. 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 individuals' decisions may be affected by cognitive biases. In consequence, they may underestimate the cybersecurity risks they face, and be over-confident that a cyber-attack will not happen to them.

Information asymmetries

In 1970, economist George Akerlof illustrated the concept of information asymmetry with the example of the used car market.[ix] The key insight is that buyers are unwilling to pay a premium for quality they can't measure. As a result of this, sellers aren't motivated to supply high-quality products.

> **There is often no easy way for a consumer to assess, prior to purchase, the level of security on a connected device**

There is often no easy way for a consumer to assess, prior to purchase, the level of security on a connected device. Often, little information on the included security measures (for example, the frequency and lifetime of product updates) is provided before purchase.

What information there is may be little more than technical jargon to many consumers (and 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[x]).

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 consequence, consumers will be unwilling to pay top dollar for a 'secure' IoT device if they have no way of verifying its level of security. And manufacturers do not have strong incentives to produce secure devices.

Misaligned incentives

A compromised consumer IoT device could have a number of implications for the device owner, including potential identity theft, fraud and the harm to property or personal security. Yet since these costs are all borne by the device owner, manufacturers do not face strong incentives to improve device 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 the functionality of the product, potentially making it less attractive to consumers.

While some firms may include better security in order to protect their brand reputation, many products in the market are white-label goods or made by relatively unknown brands, where reputational harm is likely to be of little concern.

Externalities

A compromised IoT device, service or system imposes costs not only on the user, but on the wider Internet ecosystem. As discussed earlier, if a device is compromised and becomes part of a botnet, it can be used to launch DDoS attacks, to send spam, propagate malware or to host phishing scams.

The costs of such attacks can be substantial, but in many cases, the attack target is someone other than the device owner. The insecurity in the device imposes costs on the target of the activity (and on wider society) which are not borne by the manufacturer *or* the device owner.

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.

It is also worth mentioning that there are also *positive* externalities from consumer IoT devices. These devices provide benefits to the user and positive externalities to society: for example, the adoption of energy-efficient smart devices is helping to reduce society's energy consumption.

There is a risk that security issues may deter some from purchasing devices: 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. This would mean that positive externalities from device adoption are lost.

Potential actions

As a result of these economic factors, manufacturers are likely to under-invest in security measures. 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.

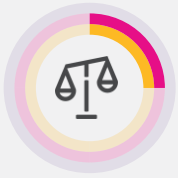
To be effective, any solutions are likely to require engagement from policymakers and industry. In addition, these solutions will have to strike a balance between improving security and allowing scope for innovation and evolution within the market, without deterring device take-up.

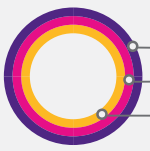
Below we suggest a number of potential actions to address the economic factors. The actions are summarised in Figure 2. They are listed in order of the likely cost and difficulty of implementing the action.

Figure 2 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, or externalities.

More detail on the potential actions – as well as a discussion of a broader set of possible mechanisms for improving consumer IoT security – can be found in the associated report.[xi]

Figure 2: Potential actions and their efficacy against the economic factors behind poor IoT security

Potential action	Efficacy against economic factors
1. Industry bodies and policymakers should raise awareness of consumer IoT security issues, and provide guidance to buyers.	
2. Governments should specify a set of security outcomes for their own procurement procedures.	
3. Industry and policymakers should encourage responsible disclosure of software vulnerabilities in consumer IoT.	
4. The industry should develop a trust mark for secure consumer IoT devices.	
5. Policymakers should require that consumer IoT devices must comply with a set of security principles (e.g. devices must be capable of being updated)	
6. Policymakers should be proactive in prosecuting manufacturers or service providers who make misleading claims on security.	
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.	



Economic factors addressed:

- Asymmetric information
- Misaligned incentives
- Externalities

Actions 1 through 6 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 (Action 7).

Action 7 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. password length).

However, while minimum security requirements are likely to reduce the risk of a device being compromised, they may also add substantially to the cost of producing devices. For example, it will cost more to provide regular software updates, or to rigorously test device security prior to sale.

Higher costs 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 advantages of better security. It may be challenging for policymakers to accurately assess these costs and benefits. As a result, it is recommended that Action 7 is employed only if other measures prove ineffectual.

Conclusion

Many consumer IoT devices have weak cybersecurity and are easily compromised. This imposes costs not only on the owners of such devices, but upon third parties and other users of the Internet.

The root cause of weak security lies in economic, rather than technical factors. Until these underlying economic factors are addressed, poorly-secured devices will continue to be produced, sold and bought.

It should also be acknowledged 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 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 therefore also be encouraged where possible.

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

About Plum

Plum is a leading independent consulting firm, focused on the telecommunications, media, technology, and adjacent sectors. We apply extensive industry knowledge, consulting experience, and rigorous analysis to address challenges and opportunities across regulatory, radio spectrum, economic, commercial, and technology domains.

For more information contact Plum at:

www.plumconsulting.co.uk

+44 20 7047 1919

[i] See 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

[ii] Hewlett Packard (2015), *Internet of Things Research Study*, http://www8.hp.com/us/en/hp-news/press-release.html?id=1909050

[iii] 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

[iv] Symantec (2018), *Internet Security Threat Report – Volume 23 (March 2018)*, https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

[v] James Scott and Drew Spaniel (2016), *Rise of the Machines: The DYN Attack was just a Practice Run*, CreateSpace, ISBN-13: 978-1540894571

[vi] For example, in 2017 this occurred with connected toys. See http://www.bbc.co.uk/news/technology-39115001

[vii] 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)]

[viii] https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

[ix] 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.

[x] An example here is ZigBee-certified products. See 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

[xi] Plum Consulting (2019), *The economics of the security of consumer-grade IoT products and services,* https://plumconsulting.co.uk/the-economics-of-the-security-of-consumer-grade-iot-products-and-services/