DAWES CENTRE FOR FUTURE CRIME AT UCL

How secure is consumer IoT?

Exploring crime associated with IoT, security features of devices and consumers' willingness to pay for security.

The 'Internet of Things' (IoT) brings internet connectivity to everyday electronic devices, allowing them to collect and share data over networks. IoT devices in the home range from speakers and smart televisions, to app-controlled burglar alarms and fridges. The IoT promises benefits in efficiency and functionality to make our homes, offices and cities 'smarter'.

IoT devices have the potential to transform society, but they also provide opportunities for crime. For example, some devices (including 'security' cameras) lack basic password functionality or allow the use of default passwords which can easily be guessed or even found in online forums. A large number of IoT devices sold to consumers lack basic cyber security provisions, leaving responsibility with the consumer to undertake tasks such as changing the default password and installing software updates. This briefing explores questions recently addressed by UCL research:

- How can consumer IoT be misused for crime?
- What security features are provided by manufacturers and what information is available to consumers?
- How do these overlap with the UK Government's 'Secure by Design' Code of Practice?
- Are consumers willing to pay for inbuilt device security?

How can consumer IoT be misused for crime?

The IoT presents substantial new opportunities for offending. To inform understanding of these risks, crimes facilitated by the IoT and the mechanisms that enable them were investigated in a systematic review of the literature. Some of the cybercrimes/harms which may be committed using consumer IoT devices are listed below. **The reader is referred to the review paper to look at the mechanisms used to enable these crimes in detail.**[4]

Key facts

15%

The number of IoT devices in the average UK household in 2020.[1]

10%

The proportion of IoT device manuals or associated online materials that advise consumers on how to secure a device from cyber risks.[2]

90%

The proportion of consumers worried about how their data is kept secure and the associated crime risks that may arise from this insecurity.[3]

Case study: The 'Miraj botnet' 2016

The first known example of consumer IoT devices being used in strategic attacks to cause disruption to online services. It targeted Internet Protocol (IP) cameras and home routers using default login credentials and infected them with the malware. These devices were combined to form a 'botnet' – a network of compromised devices – and used to launch Distributed Denial of Service (DDoS) attacks.[5] DDoS attacks make services like websites unavailable by overwhelming them with traffic from multiple sources.

Key facts

52%

The proportion of consumers who regularly download the latest software updates for their mobile phones, desktops and laptops.[6]

32%

The proportion of consumers who follow the latest government password advice.[6]

4

The average number of security features available per device.[2] While the quality of features is more important than quantity, Government guidance recommends 13 features.

Energy theft: Use of smart meters or other devices to steal electricity, manipulate energy costs in distribution networks, impact smart grid networks or cause blackouts.

Burglary: Information from devices can reveal household occupancy based on user activities (i.e. 'profiling'). Further exploitation of connected devices such as smart locks can allow attackers to gain physical entry.

Sex crimes: Use of devices to facilitate sex-related crimes including stealing sex-related videos, transmitting obscenity and voyeurism.

Political: Exploiting devices for political gains (such as political control and propaganda).

Identity theft: Stealing sensitive personal information from devices to commit identity fraud.

Harm to inhabitants: Causing physical or mental harm to individuals including vulnerable groups (such as children and older adults) who may be susceptible. For example, targeting devices with heating capabilities to cause a fire in the home.

Misinformation: Use of devices to give false or inaccurate information (such as a false fire alarm).

Profiling, targeted or unsolicited advertising: Use of information from devices for targeted advertising or marketing.

Blackmail: Use of information gained from devices to blackmail individuals.

Vandalism: Damage to physical property or household objects arising from exploited devices with actuators (mechanical components that affect the environment).

Discrimination: Use of information from IoT devices (such as beliefs or health information) to discriminate against individuals.

Stalking: Use of information gained from devices (such as location) to stalk people.

Code of Practice for consumer IoT

In response to DDoS attacks such as the Mirai botnet, there has been a recent push by governments and security experts to motivate manufacturers to build security into products, making them 'secure by design'. In March 2018, the Department for Digital, Culture, Media and Sport (DCMS) introduced the Secure by Design Code of Practice (CoP). It outlines 13 principles that manufacturers should follow to achieve good security.[7] The Government opened a call for views[8] in summer 2020 on regulating the first three of these: (1) Ban universal default passwords in consumer smart products, implement a means to manage reports of vulnerabilities, and thirdly to provide transparency on how long products will receive security updates.[8]

Alongside this, the Government published commissioned research by the CSES on the nature and scale of cyber security vulnerabilities in the IoT landscape and by RSM on evidencing the cost of the planned interventions. The proposed regulation will follow the European Telecommunications Standards Institute (ETSI) European Standard (EN) 303 645 v2.1.1, published in June 2020.[9]

Security features of consumer IoT

The IoT is recognised as being widely insecure, in large part due to the lack of security features built into devices. When security features are available, consumers do not always use them. It is also hard for consumers to ascertain what security devices provide before purchase. The table below shows what information is communicated to consumers. The figures are based on information extracted from device manuals and online materials in 2018 for 170 devices (searches were conducted for a further 100 devices but no online materials could be found).[2] These devices may have further inbuilt features, but information about these was not available to consumers prior to purchase. It is also possible that fewer features were provided for the 100 devices for which no information was available.

The most commonly referenced features in manuals were account management and software updates. However, they were mostly discussed in terms of product use and maintenance or functionality rather than product security. For example, considering the third point in the CoP (keep software updated) in particular, while this was frequently discussed, it was only described in relation to security in 10% of cases. In addition, none of the materials reviewed detailed for how long security updates would be provided.

78%	Devices are not shipped with **default passwords** and require credentials to login
77%	**User account management information provided** (such as password protection and password reset)
62%	**Software and firmware updates offered**
48%	A **factory reset** option is available
32%	The manufacturer had a **vulnerability disclosure policy** in place
20%	**Wi-Fi encryption standards** are discussed
17%	**Data encryption** in motion [rather than stored on the device]
17%	Product can be **locked** to prevent unauthorized access
15%	Encryption at rest (when data is stored on the device)
10%	Cyber hygiene advice given to encourage cybersecurity behaviour
10%	Additional privacy features discussed that help to protect the privacy of the device, such as limited location sharing
8%	Owner could delegate or revoke **permissions** for use and access to data stored on devices
5%	**Security of the cloud services** the product uses discussed
5%	Information provided about **local communications encryption**
3%	Data only stored on the device **locally**
2%	User was encouraged to use **two-factor authentication** to secure online accounts

Secure by Design Code of Practise for consumer IoT.[6]

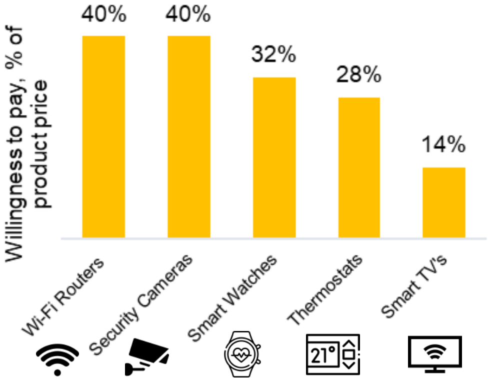
1. No default passwords
2. Implement a vulnerability disclosure policy
3. Keep software updated
4. Securely store credentials and security-sensitive data
5. Communicate securely
6. Minimize exposed attack surfaces
7. Ensure software integrity
8. Ensure that personal data are protected
9. Make systems resilient to outages
10. Monitor system telemetry data
11. Make it easy for consumers to delete personal data
12. Make installation and maintenance of devices easy
13. Validate input data

References

1. Wrap (2017). Smart Devices and Secure Data Eradication. https://www.wrap.org.uk/content/smart-devices-secure-data-eradication-evidence
2. Blythe, Sombatruang & Johnson (2019). What security features & crime prevention advice is communicated in consumer IoT device manuals & support pages? https://academic.oup.com/cybersecurity/article/5/1/tyz005/5519411
3. The Economist Intelligence Unit. (2018). What the Internet of Things means for consumer privacy.
4. Blythe, J.M., Johnson, S.D. A systematic review of crime facilitated by the consumer Internet of Things. Security Journal (2019). https://doi.org/10.1057/s41284-019-00211-8
5. BBC News. (2017). Mirai botnet: Three admit creating and running attack tool. Retrieved from http://www.bbc.co.uk/news/technology-42342221
6. Office for National Statistics (2016). Crime in England and Wales: Year Ending Sept 2016. England, UK.
7. DCMS (2018). Secure by Design COP. Available at: https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security
8. DCMS, 2020. Proposals for regulating consumer smart product cyber security - call for views and supporting research. Available at: https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views
9. ETSI EN 303 645 v 2.1.1. (June 2020). Cyber Security for Consumer Internet of Things: Baseline Requirements. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
10. Blythe et. al., (2020). What is security worth to consumers? Investigating willingness to pay for secure IoT devices. https://link.springer.com/article/10.1186/s40163-019-0110-3
11. Johnson et al. (2020). The impact of IoT security labelling on consumer product choice and willingness to pay. https://doi.org/10.1371/journal.pone.0227800
* Chart icons made by Freepik.com from https://www.flaticon.com/

What is security worth to consumers?

Added security comes with an increased cost to manufacturers. This work[10,11] found that consumers would be willing to pay more for added security, but the amount depends on the type of device. The chart* shows estimates of the proportion of the product price that consumers would be willing to pay.



However, willingness to pay is not dependent on the level of risk reduction offered, suggesting that consumers would not pay more for a higher reduction in risk.[10]

Policy implications

This work has implications for consumer IoT security and the implementation of the CoP. It has already informed the UK Government's Secure by Design agenda and helped to explore policy options for addressing vulnerabilities in consumer IoT, including a potential security labelling scheme.[10,11]

The IoT offers potential for new types of crime. Preventing such crimes should involve opportunities for consumers to make their devices secure, either via regulation or a labelling scheme and through greater security by design. Secondary to this is exploring consumers' capability, motivation and opportunity to protect their devices and themselves, with awareness raising interventions designed accordingly.

Consumer IoT device manuals, or other materials available prior to the purchase of devices, do not currently provide adequate information about security features. Available security features should be summarised in an accessible format to assist consumer purchasing choices, and to enable scrutiny from security professionals and consumer advocacy groups. Consumers are willing to pay for inbuilt device security, which indicates the importance of ensuring security by design and the role of manufacturers in addressing this problem.

Our research

This work was carried out by the Dawes Centre for Future Crime at UCL. This briefing was produced in partnership with Florence Greatrix at UCL STEaPP's Policy Impact Unit. The research was funded by the Dawes Centre for Future Crime at UCL and the PETRAS Internet of Things Research Hub.

Lead researchers

Professor Shane Johnson, Principal Investigator, Dawes Centre for Future Crime shane.johnson@ucl.ac.uk
Dr John Blythe, CybSafe, john@cybsafe.com
Professor Matt Manning, Australian National University, Matthew.Manning@anu.edu.au
Dr Gabriel Wong, Australian National University, Gabriel.Wong@anu.edu.au

Contact us

https://www.ucl.ac.uk/jill-dando-institute/research/dawes-centre-future-crime
https://www.ucl.ac.uk/steapp/collaborate/policy-impact-unit-1