Connected toys and the Internet of Things

The new risks

Connecting products to the internet brings tremendous benefits. Whether it be fitness bands collecting movement data to help you exercise or home energy meters monitoring the electricity used to make you more efficient, the benefits are as innumerable as they are amazing. Not surprisingly many are predicting enormous growth in the IoT sector, with the market expected to be worth 318 Billion USD by 2023[1].

The toys and children's products market is expected to follow this trend, taking a sizeable 18 Billion USD chunk of that market[2]. The innovative and highly competitive toys market is already making use of these new technologies, with more than twice as many companies producing connected toys in 2018 vs 2019[3].

New Technologies, New Risks?

As with any new technologies, the risks need to be properly considered as they are implemented. The toy industry is very serious about the safety of children; connecting toys to the internet may present new risks of harm to children that everyone needs to be aware of. Aside from that, connecting any product to the internet brings potential risks of the loss of personal data, some of which might be sensitive. There are also risks to the very infrastructure of the internet itself.

[1] https://www.windpowerengineering.com/business-news-projects/global-iot-market-to-reach-318-billion-by-2023-says-globaldata/

[2] https://www.juniperresearch.com/press/press-releases/smart-toy-revenues-grow-almost-200pc-by-2023

[3] http://www.collabsco.com/perspective

What are the risks?

The risks come in three forms “Cyber security, Data Privacy and Product safety”.

Data Privacy is the ability of an organisation to keep information, usually regarding an individual or group of individuals, private. So, for connected toys, it is about making sure that personal information is kept private. This is regulated by the GDPR and has been in the news a lot recently. There are several stories about big companies potentially having to pay huge fines for losing data.

Cybersecurity is the act of protection against the criminal or unauthorised use of electronic data, or the measures taken to achieve this. Perhaps the biggest risk of connecting products to the internet is the potential loss of control. Malicious actors can seek to remotely gain control of the device and make it operate in an unintended way. The risks become more serious when presented with a large group of connected products, controlled simultaneously these could potentially overload national infrastructure (e.g. if all thermostats were operated at the same time it could cause serious issues in the national electricity and gas networks). Using computer viruses, hackers can “recruit” devices into a “botnet”, a network of devices that can be programmed to send thousands of electronic communications to a single computer or network. The Mirai botnet attack in 2016 managed to shut down major service providers such as Twitter and Spotify[4].

[4] https://www.bbc.co.uk/news/technology-37738823

We think product safety issues are well understood for toys, however, connected toys pose new challenges. There have been no publicised examples but changing a product's software could change the way it behaves. With the frequent need to update software for security reasons, unless the updates are fully tested before being sent to devices, it is possible it could cause them to malfunction.

Addressing the risk

Fortunately, there is now lots of guidance on what the technical risks are and how they should be controlled.

The key security issues are still somewhat basic. The Open Web Application Security Project (OWASP), whose members include security experts from around the world, published a top ten of things to avoid when building, deploying, or managing IoT systems[5]. Top of the list is still "weak passwords" yet there are now well know techniques to control this.

In October 2018, the UK Department for Digital, Culture, Media and Sport (DCMS) issued an IoT Code of Practice for industry containing 13 high level topics for connected devices. The DCMS worked with international standard organisation, ETSI, to produce a standard for cybersecurity in the Internet of Things[6], which is freely available.

OWASP Internet of Things (IoT) Top 10 2018

I1 Weak Guessable, or Hardcoded Passwords

I2 Insecure Network Services

I3 Insecure Ecosystem Interfaces (the link between two or more pieces of hardware or software systems e.g. running a document editor software with some cloud storage software to edit online)

I4 Lack of Secure Update Mechanism

I5 Use of Insecure or Outdated Components

I6 Insufficient Privacy Protection

I7 Insecure Data Transfer and Storage

I8 Lack of Device Management (ensuring only authorized devices are connected to a network and that they stay authorized or are removed)

I9 Insecure Default Settings

I10 Lack of Physical Hardening (physical security which can include being able to upload software via USB key or even being able to read a password on a home router)

[5] https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10

[6] https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security

The 13 topics in the ETSI standard

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. Minimise exposed attack surfaces

7. Ensure software integrity

8. Ensure that personal data is protected

9. Make systems resilient to outages

10. Monitor system telemetry data (Ensure the transferred data is within set parameters – unexpected data can be indicative of an attack)

11. Make it easy for consumers to delete personal data

12. Make installation and maintenance of devices easy

13. Validate input data

Following these guides is a good way to ensure most of the risks are addressed. Toy companies will normally be relying on external expertise for things like app or website design, so it is important to use specifications like the ETSI standard as a means of describing the requirements. There are also numerous tools available on the OWASP website.

Also consider some third-party security testing. Just as toy companies have products tested against the product safety standards, the same considerations should be made for cybersecurity. Expert help is available to perform "penetration testing" to look for potential vulnerabilities before the product is placed on the market

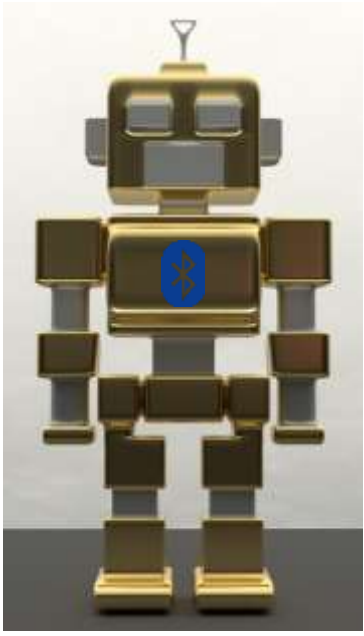
BTHA guidance

The BTHA guidance is evolving and has recently been updated to reference the new external guides and requirements. The BTHA guide also includes a checklist of requirements and issues to be addressed, broken down over a product's typical development cycle. It even includes things to consider when distributing a third-party product. Members enjoy the benefits of having experts to help direct them to right resources for help.

The connected toys guidance was first published back in 2017, one of the first consumer product sectors to do so. It has set the scene for other

guides and publications that we see published today. The guidance is constantly being evolved as the busy regulatory landscape shifts.

Regulatory activity



Since the risks involve the security of the internet infrastructure, it is little wonder governments are taking this seriously. A UK government report on Security by Design[7] from March 2018 points out:

> *Cyber criminals could exploit vulnerabilities in IoT devices and associated services to access, damage and destroy data and hardware or cause physical, or other types of harm. Where these vulnerabilities can be exploited at scale, impact could be felt by multiple victims across geographic boundaries*

The UK government is leading the way in Europe in terms of regulation. Having published their Cyber Security Code of practice in October 2018, they have recently consulted on ways to make the top three points mandatory requirements. The same goes for data Privacy, with the UK Information Commissioners office (ICO) flexing their muscles in the implementation of the GDPR:

> *"People's personal data is just that – personal. When an organisation fails to protect it from loss, damage or theft it is more than an inconvenience. That's why the law is clear – when you are entrusted with personal data you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights." - Elizabeth Denham CBE, Information Commissioner.*

The ICO are currently consulting on a set of requirements on the "age appropriate design" of websites, apps and connected toys, that would demand companies set websites and apps used by children to high privacy by default as well as a number of other requirements for communicating with children, that could require significant changes for UK and foreign companies operating in the UK.

[7] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775559/Secure_by_Design_Report_.pdf

Regulatory activity

October 2018 – DCMS CoP produced

March 2019 – ETSI TS103 645 on Cyber Security published

May 2019 – DCMS consults on mandatory Cybersecurity requirements

May 2019 – ICO consults on age appropriate design requirements

June 2019 – EU Cybersecurity Act Published

2019-2020? – Internet Certification requirements

Also look out for the European Cybersecurity Act. This act gives the EU Cyber security Agency (ENISA) the power to regulate internet connected products. ENISA say they plan to start setting mandatory certification requirements for connected products in late 2019 to early 2020.

What Next?

Cybersecurity and Data Privacy are clearly two very important topics for the regulators and for the public too. As the IoT market grows, so will consumer concerns about the security of their products. The technology looks ripe for innovation by the toy industry into a new wave of exciting toys, but developers clearly have responsibilities to their consumers, all under the watchful eyes of the regulators. Provided manufacturers are aware of the risks, as highlighted by the guidance that is available, the risks should be easy to control.

Written by Antony Kirrane, one of the BTHA compliance team and connected toys expert. Members can access the BTHA guidance from the guidance section of the website