nccgroup

Shutterstock Credit ID: 1095960386

Dec 10, 2019 05:19 GMT

A technical review of connected toy security

Overview

In the run up to Christmas 2019, the consumer choice organisation Which? engaged us to assess the security of seven popular electronic and connected toys. This is an activity that Which? has performed across a few years, so this time round provided an opportunity to see if any security improvements had been made across the connected toy industry in relation to preservation of the privacy and safety of children.

Our security assessment focused on:

- The confidentiality of any personal data captured and processed by the toys
- The integrity of any data captured and processed by the toys
- The availability or correct operation of the toys

Contextually, our assessment also focused on any exploitable or design-based technical issues specific to the use of the toys by children. This included whether vulnerabilities could be used to exploit or harm children in any way, particularly in instances where the toys were likely to be used in environments without direct parental supervision.

Across all seven toys we found 20 noteworthy issues – two were high risk, three were medium risk and the remainder were low risk.

In this blog post we present these common issues and themes in order to highlight the security improvements connected toy manufacturers need to make.

We hope that this blog post also helps to educate parents and guardians and enable them to make informed risk-based decisions when purchasing connected toys.

What is a 'connected' toy?

Before we dive into the issues identified during our security assessment, it's worth defining what we mean by 'connected' toy. The idea behind a connected toy is good – electronic and IT capabilities are used to take the concept of a toy away from an inanimate object, and to give it some capability to interact with a child.

The connected aspect could include localised electronic connection, such as Bluetooth, to an app running on a smart device, or direct connection to the Internet via connection to a home Wi-Fi router. The interfaces in the toy could include microphones and cameras to receive audio and visual inputs from a child, and loudspeakers and screens for feeding back audio and visuals to the child as part of some form of interaction.

Usually the connected or online aspect is used to simulate an element of intelligence or evolution in the toy. For example, a child may be able to ask it questions, which without the child knowing, enables the toy to perform an internet search and speak back the results to the child. Other common implementations include evolutionary traits, whereby the toy could learn or acquire new skills and functions by learning from interactions with a child, or updating itself with new features and behaviours via app or internet connectivity.

For connected toy manufacturers, the possibilities are endless, restricted only by aspects such as cost of production and time to market. From NCC Group's experience, it is these two aspects that likely dictate the low levels of security commonly observed in connected toys.

The cost of getting this wrong however, on top of potentially exposing or harming children could also be at the detriment to the toy manufacturer as a result of legal or regulatory fine, or significant drop in market potential. This has already happened in Germany [1] where in 2017 the Federal Network Agency announced a ban on certain connected toy types (famously the 'Cayla Doll' [2]) that could present 'spying capabilities' against vulnerable children.

Below we highlight common themes observed from our recent security research across the seven toys provided by Which?.

Websites, apps and online forums

Many of the toys either required or suggested the creation of an online account. The use-cases differed per toy, but usually this was required or suggested in order to register the toy, allow children to download new capabilities, or to share aspects or experiences with the toy in online forums with other children.

For example, some of the toys could be programmed using high-level or graphical languages that would make the toys perform specific tasks which could be shared in online forums. We presume that toy manufacturers would use account information and authenticated users for data analysis and marketing purposes – later we highlight some observations and concerns from a privacy policy perspective regarding the nature and intention of the data captured by many of these online systems.

We note that some of the account creation functions did require parent or guardian input and authorisation. Enforcing this, however, is not possible across the internet. and so those children old enough to be able to use computers and create online accounts would be able to do so without adult consent. Age verification of children online is currently a topic of high priority in the UK in relation to a broader drive to reduce online harms [3] and NCC Group is currently engaged in a several activities aimed at deriving solutions in this space.

Security testing of the websites and online forums was not in scope of this toy security investigation, however, from observation of normal operation and use, we commonly observed:

- Plaintext logins and authenticated sessions – there was no encryption on account creation and account logins, meaning that the usernames and passwords and all associated account and session information on some toy websites and forums, was open to interception.
- Username and email address enumeration – when creating new accounts, or using the 'forgotten password' function, the websites commonly returned messages that would indicate whether a given username or email address was already registered. Attackers would be able to perform a brute-force attack against these functions to enumerate valid usernames and email addresses registered on the sites.
- Weak password policies – none of the websites enforced a password policy. On all of them, it was possible to set a password of 'password' which is incredibly weak and highly guessable. This lack of a password policy, coupled with the username and email address enumeration issue could be used by attackers to successfully brute-force valid username and password pairs to gain unauthorised access to user accounts.

Where online access provided forums for children to share data or experiences regarding their toys, we also observed minimal moderation or censorship capability within the websites, meaning that offensive content could be shared in some forums (visual, textual or audio). Some of these forums did offer a mechanism to report offensive content, however this would be a reactive rather than pre-emptive approach.

Online privacy policies

NCC Group's privacy experts were engaged to review the privacy policies of the various websites and forums relating to the toys under investigation. Common observations here included:

Even though there was no specific requirement or need to set up an online account and provide personal data for normal toy use and operation, the option to do it existed which means compliance with the General Data Protection Regulation (GDPR) [4]/Data Protection Act (DPA) 2018 is necessary in the UK, but was not necessarily reflected in the privacy policy of the website.

The policies were commonly found to be vague, and arguably not complying with the Children's Online Privacy Protection Rule (COPPA) [5] requirement for there to be a 'clear and comprehensive online privacy policy'. COPPA imposes certain requirements on operators of websites or online services directed at children under 13 years of age. Our findings regarding username enumeration and weak password policy highlighted failings of the COPPA requirement.

It was unclear why many websites needed to collect a child's gender and date of birth.

Many of the websites were also not complying with the Privacy and Electronic Communications Regulations (PECR) [6] on cookies and approaches seen on the websites to getting users to disable or reject them is not good practice. We saw policy text such as 'We collect information passively. We use tracking tools like browser cookies and web beacons to collect information from you.' Also in relation to PECR, some websites were not clearly stating that they would not send anything to children.

Device pairing – missing authentication

Many connected toys need to pair with some other device, whether with another toy (such as a pair of walkie talkies) or with a mobile device running a specific app. Bluetooth is commonly used for localised connection, usually within 10 meters, or perhaps further with Bluetooth Low Energy (BLE). A key observation with Bluetooth used for toy pairing, is lack of authentication

where there is no need to enter a session-based PIN. The reasons for not implementing authentication are understood, such as ease of operation –especially for children – and minimal or missing interfaces present on toys that might be needed to display a unique pairing code for example. However, the consequences of not authenticating Bluetooth or similar connections could be abused in a number of ways when the context is use by children:

- Offensive content – two of the toys investigated were karaoke toys, allowing audio to be streamed to them via Bluetooth. Anyone within range of these toys would be able to anonymously pair with them and start streaming audio into them, which could perhaps be offensive in nature.
- Child manipulation – even though the karaoke toy Bluetooth connections were one-directional, it's possible to imagine a scenario where someone connects to the toy and streams instructional or manipulative messages to a child, such as asking them go out to the front garden, as a precursor to an abduction attempt.
- Two-way child interaction – a pair of walkie talkies investigated as part of this security assessment allowed for children to communicate with each other, within a range of up to 150 meters. There was no mutual authentication between the pairs of walkie talkie devices. This means that if an attacker purchased the same set of toys and was in range of an unpaired, powered-on walkie talkie, they would be able to successfully pair with it and engage in a two-way conversation with the child user under certain conditions.

Toys used in second-order IoT attacks

Another observation from our security investigation was the potential exploitation of some of the toys as part of a second-order IoT attack against emerging smart homes [7]. In second-order IoT attacks, IoT devices are used or exploited as a conduit to exploiting a secondary device or system.

For example, with the two karaoke toys investigated and their unauthenticated Bluetooth implementations, it was possible to connect to them when in range and issue digital assistant voice activation commands.

While different smart home configurations will exist, it is not inconceivable

that some homes might have digital assistants configured to open smart locks on front doors, for example. One can thus imagine an attacker outside of a property, connecting without authentication to a Bluetooth toy to stream audio commands to enact a second-order objective, such as “Alexa, unlock the front door” [8].

Recommendations to connected toy manufacturers

There are a number of steps that toy manufacturers should follow to improve the security of connected toys and associated internet-based components, in order to preserve the privacy and safety of children.

- Where Bluetooth or similar device-to-device pairing is used, manufacturers should seek to implement authentication and authorisation between toys and their owner devices and controlling apps. This is required to prevent attackers within vicinity attempting to interact with children via Bluetooth or similar local radio-based interfaces, and to protect smart homes from second-order IoT attacks.
- While connected toys may expose minimal interfaces, there are still methods that could be employed with those minimal interfaces to implement improved authentication and authorisation:
- Where toys have a mechanism for persistent storage, this could be used to store some unique identifier of a controlling app upon first use. For example, a toy owner’s Bluetooth audio streaming device might generate a unique ID which is transmitted to the toy and stored within the toy. Upon each subsequent toy-app connection, the toy could check that the connecting device/app is that of the owner.
- Where toys have a mechanism to display text or project audio through a loudspeaker, this could be used to present a random one-time pairing code which changes upon each connection, and must be typed into the user’s mobile app. This type of operation would ensure that both toy and controlling mobile app mutually authenticate each other and make it difficult for someone in the vicinity to guess the randomised pairing code for unauthorised toy connectivity.
- When toys implement local radio-based pairing with other devices, manufacturers should implement a timeout and auto-power-off after a pre-defined period (e.g. 5 minutes) of inactivity.

Automatically powering off unattended toys will minimise the potential for unauthorised individuals within range to connect to them.

Any websites or applications created and maintained by toy manufacturers should be developed with strong security in mind, ensuring compliance with all relevant standards, regulation and legislation including GDPR, COPPA, PECR, with regards to data protection. Strong password policies should be enforced and strong encryption (TLS) should be enforced on all authenticated sessions, while username and email address enumeration should be avoided through use of appropriate error messages and use of components such as CAPTCHAs [9] during account registration.

Where online forums offer chat or data sharing functions, blacklists (while not exhaustive) of offensive words and content should be used against all uploaded or typed content. Where graphical, audio or video imagery can be uploaded and shared, moderation processes should be in place and enforced before content is published to all. Similarly, mechanisms for reporting offensive content should be implemented and made clearly available on the underlying website/forum.

The EC JRC Technical Report – Kaleidoscope on the Internet of Toys [10], and the Digital, Culture, Media and Sports (DCMS) Code of Practice for Consumer IoT Security [11] are a must read for any connected toy manufacturer.

Guidance for parents and guardians

While the onus should never fully lie with parents or guardians, checking that the product literature has sufficient reference to security and privacy before purchasing should be the first step. And if concerns persist after purchasing the device, supervision should always be performed on toy operation and any accompanying online activity and use.

To mitigate issues around Bluetooth exploitation, parents should encourage behaviours in children to ensure all electronic devices are turned off when not in use. Powered-down devices cannot be exploited. If children are too young to remember or perform the powering-down of devices, then parents should ensure this occurs when the toys are not in use.

Supervision is also recommended, at least initially, on any online account creation and use. Parents and guardians should familiarise themselves with the websites and applications that may be necessary for toy operation, and be aware of any potential for child interaction through online chat forums or any potential for viewing of offensive/inappropriate material. For younger children, use of online resources under constant parental supervision or in communal areas within households is recommended.

How NCC Group can help

NCC Group has a wealth of experience in IoT security. We work with IoT manufacturers at all stages of development, from secure product design through to security testing of final products.

We have published guidance in this domain [12] and regularly speak at international conferences and seminars on IoT security and best practice.

Our IoT consultancy and testing spans all aspects of the IoT ecosystem, from low-level hardware secure design and testing via our specialised hardware labs, to cloud-based testing of web services that consume and process hundreds of thousands to millions of IoT device events.

We also work with manufacturers on implementing and/or improving the security of their Software Development Lifecycles (SDLC), while we also work with those needing assistance with incident response and how to triage and remediate incoming reported vulnerabilities in IoT products and systems.

References

[1] https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/14012017_cayla.html?nn=265778

[2] https://www.bbc.co.uk/news/world-europe-39002142

[3] https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper

[4]

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

[5] https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

[6] https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/

[7] https://www.nccgroup.trust/uk/our-research/using-graph-databases-to-assess-the-security-of-thingernets-based-on-the-thingabilities-and-thingertivity-of-things/

[8] https://support.smartthings.com/hc/en-gb/articles/115003111686-How-to-connect-locks-to-Alexa-with-SmartThings

[9] https://www.owasp.org/index.php/Testing_for_Captcha_(OWASP-AT-008)

[10] https://publications.jrc.ec.europa.eu/repository/bitstream/JRC105061/jrc105061_final_online.pdf

[11] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

[12] https://www.nccgroup.trust/uk/our-research/security-of-things-an-implementers-guide-to-cyber-security-for-internet-of-things-devices-and-beyond/

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted

by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

NCC Group - Financial Media Enquiries
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750