TOP 10 VPN

Report:

Assessment of the Privacy and Security of Smart Toys Marketed to Children

8 December 2017 (Redacted version)

Conducted by

Sarah Jamie Lewis
Independent Security Researcher
Mascherari Press

sarah@mascherari.press

Commissioned by

Simon Migliano
Head of Research
Top10VPN.com

simon@top10vpn.com

Summary

We assessed the privacy and security of six different toys and devices marketed to children. We were able to compromise all of these devices and found critical vulnerabilities that could impact the security or safety of a child in five of these devices.

Issues that we found that could endanger children included: interception of the camera or microphone inside the toy, the ability to retrieve private pictures and video from the device, the ability to intercept the location of a device and the ability to spoof information such as child location to a parental monitoring app.

This report provides details of our assessment methodology, a general analysis of our results as well as redacted reports of each product tested - pending manufacturer notification, and potential fixes.

Introduction

In recent years the number of consumer products marketed to children that require or include access to the internet has grown exponentially. This project assessed a selection of these consumer products in order to determine if manufacturers are taking the privacy and security of these products as seriously as they should be.

Methodology

Each product underwent a variety of assessments designed to test their privacy and security.

- Passive Network Monitoring - Each major product feature was triggered and any networking traffic recorded for examination of privacy and security issues. This phase assessed:
  + If the product used Bluetooth, WiFi and/or other kinds of radio communication.
  + If encryption is being used by the product and any associated applications, and if the encryption being used is sufficient to maintain privacy and security.
  + If data being sent by the application is vulnerable to network interception.
- Active Application Security Assessment - A selection of features of each product underwent further testing to ensure they are not vulnerable to being actively exploited by an adversary. This step examined:

  - + If the product had any security issues which may endanger the safety or privacy of a user.

- Data Collection, Privacy Policy and Disclosure Assessment - For each product we examined the data being collected during setup (both explicitly in registration forms and implicitly as derived from the passive network monitoring and by reviewing the privacy policy) to ensure:

  - + That the data being collected is reasonable and appropriate
  - + That the data being collected is explicitly referenced in the privacy policy.

General Analysis

While we assessed many different types of toys and devices, we were able to make some general assessments regarding their security and privacy.

Bluetooth v.s. WiFi

While none of the Bluetooth or WiFi toys toys we examined were immune to being compromised by an attacker, the impact of such a compromise can clearly be differentiated between the two communication mechanisms.

While Bluetooth as a technology supports secure pairing, the Bluetooth toy we examined did not make use of this feature, which is common. However, Bluetooth tends to be used in toys that require relatively low power, and as such these devices have limited capabilities e.g. they lack a camera and a microphone.

On the other hand, we examined many different devices that all setup their own WiFi hotspot that a user was required to connect to. These devices require a WiFi connection in order to support more features such as video sharing.

We were able to compromise all of the WiFi devices we examined and because of this increased feature set the compromises were more serious.

This distinction provides an important insight for anyone wondering about the security of a device - Bluetooth devices, on average, are less risky devices - even if they are just as easily compromised as WiFi devices.

The Dangers of Video Streaming Devices

We assessed three different devices that offered some kind of video streaming, and without exception we were able to compromise and intercept the video stream from the device.

All of that devices that supported video streaming required an onboard WiFi hotspot to transport it - appropriate security measures on this WiFi connection would have mitigated the video interception vulnerabilities, yet only one of the manufacturers required a password to connect to the WiFi hotspot, and this password was hardcoded, the same across all devices and easily looked up online.

The Insecurity of Firmware Updates

Most of the toys that we looked at provided a mechanism for updating the firmware onboard the toy. While every toy had a different update mechanism we found all of them to be flawed, often making it trivial for an attacker to damage a device or, with more skill and effort, install malicious software onto the device itself.

Childrens Tracking Watches

The security and privacy of smart watches designed and marketed to be worn by children has been the subject of recent media attention.

We analyzed the Q50 smart watch and found similar worrying vulnerabilities which would allow an attacker to secretly monitor the child’s conversations, spoof the location of the tracking watch as well as interception and learn the child’s location and update and delete safety numbers on the phone.

It seems very clear that the approach taken in Germany of restricting the purchase of these watches is justified, it is hard to see how these products do not endanger the safety of the children who wear them.

Product Report: Q50 Smart Tracking Watch

The Q50 is is a smart watch designed for children. Allowing guardians to track the child's location, send messages, remotely monitor the child's surroundings and conversations and receive SOS alerts from the child among other features.

Security Summary

Security	Privacy	Danger
🔴●●	🔴●●	🔴●●

If the watch was in use by a child the security and privacy flaws with this device would allow an attacker to intercept all communications, remotely listen to the child's surroundings and spoof the child's location.

The watch has an SMS control channel that is protected by a password. Unfortunately the default password is 123456 and users are not prompted to change this at any point.

Once the number associated with the watch is known, the attacker can send commands to the watch which include activating the remote monitoring mode and listening to everything the wearer says.

Further the protocol used by the watch to communicate with the server provides no authentication or authorization protection. This means it is possible for anyone who knows the ID of the watch to spoof the watches location as well as spoof messages / SOS alerts.

The attacker can also lock out the primary monitoring accounts, reconfigure all settings and otherwise turn the device against the device's owners.

This device is fundamentally not secure and to use it potentially endangers the child compared to not wearing a tracking watch at all.

Even if the control channel password was changed, the hard limit of 6-digit for the password is trivial to bruteforce.

We also identified other privacy and policy related issues such as the inclusion of over a dozen different advertisement and tracking scripts within the companion application - however, compared to the issues identified above, these are minor.

Product Specifications

Connectivity	GSM (SIM Card not Included)
Camera	No
Microphone	Yes
Additional Data Collection	The app collects Child Name, Sex, Parents/Guardian phone numbers, Text/Voice messages between the App and the Watch

Product Report: Mass Effect: Andromeda NOMAD ND1 RC Car

The NOMAD ND1 is a remotely controlled toy car which is controlled through a mobile app (available for both Android[1] and iOS[2]).

Security Summary

Security	Privacy	Danger
🔴 ⚫ ⚫	🔴 ⚫ ⚫	🔴 ⚫ ⚫

We found multiple issues impacting the security and privacy of this product. These vulnerabilities would allow an attacker to take complete control over the car and intercept the video stream from the built in camera.

In addition we discovered an issue that would allow an attacker to render the device inoperable - or allow them to install other kinds of malicious code on the device.

The one mitigating circumstance for all of these vulnerabilities is that an attacker must be in range of the device.

We found no issues with the companion app, or the related privacy policies.

Product Specifications

Connectivity	WiFi (802.11G Channel 9 used only) - No Authentication
Camera	Yes
Microphone	No
Additional Data Collection	None

[1] https://play.google.com/store/apps/details?id=com.pdp.MEAndromeda&hl=en

[2] https://itunes.apple.com/us/app/mass-effect-andromeda-nomad-nd1-r-c-app/id1168112182?mt=8

Product Report: Sky Viper v2400 HD Streaming Drone

The Sky Viper v2400 HD Streaming Drone is a remote controlled drone with a built-in camera. The drone is controlled via a controller. Video and pictures from the device can be streamed with a companion application that is available for both Android[3] and iOS[4].

Security Summary

Security	Privacy	Danger
🔴 ● ●	🔴 ● ●	🔴 ● ●

We found multiple issues impacting the security and privacy of this product.
These vulnerabilities would allow an attacker to intercept live video from the drone, access previously captured pictures and video, lock users out of their device as well as potentially damaging the device.

All of the attacks that we found require an attacker to be within range of the WiFi network that the device creates.

We found no issues with data collection or privacy policies relating to the companion application.

Product Specifications

Connectivity	WiFi (No Authentication) - Video Stream Radio - Controls
Camera	Yes
Microphone	No
Additional Data Collection	None

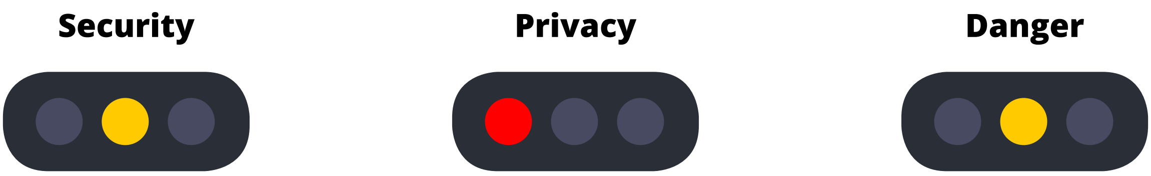
[3] https://play.google.com/store/apps/details?id=com.newskyviper&hl=en

[4] https://itunes.apple.com/ca/app/sky-viper-video-viewer/id1004871562?mt=8

Product Report: AirHogs FPV High Speed Race Car

The AirHogs FPV Race Car is a radio controlled car that also is sold with a headset which the user can insert a phone into and get a first-person view through the car's camera. The video stream can be accessed, edited and the results shared through the Android[5] and iOS[6] applications.

Security Summary



The controls and video feed for the AirHogs Race Car are delivered over separate channels - with a radio link being used for car control, and a WiFi network is setup and used to deliver video.

While it is unlikely that the split between radio controls for the product's movement and WiFi transported video stream provides any real security benefits against a determined attacker, it likely provides some practical defense against casual threats.

It is trivial to intercept video from an AirHogs Race Car for an attacker in range of the onboard WiFi.

Product Specifications

Connectivity	WiFi (No Authentication) - Video Stream Radio - Controls
Camera	Yes
Microphone	No
Additional Data Collection	None

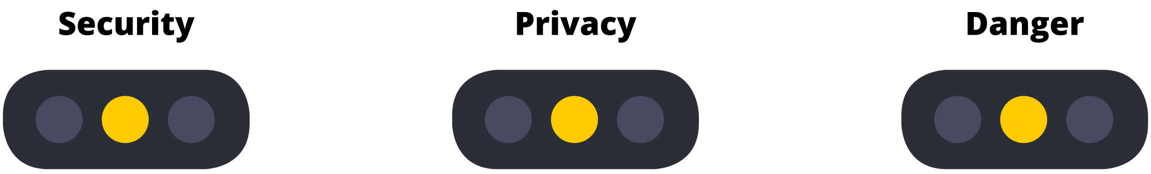
[5] https://play.google.com/store/apps/details?id=com.spinmaster.airhogs.fpvcar&hl=en

[6] https://itunes.apple.com/us/app/air-hogs-fpv-race-car/id1276733501?mt=8

Product Report: CogniToys Dino

Dino is an internet connected educational toy designed for children. The Dino listens and responds to children's questions, plays games and has many other features. While an android or iOS app is required for setup, it is not required afterwards.

Security Summary



We found privacy issues with Dino which raise concerns about the security of the device.

Dino transmits a variety of information, though as far as we can tell no information provided by the child, over the internet unencrypted.

The device also appears to rely on unencrypted network connections to set up the device as well as to deliver firmware updates.

While these flaws require a more sophisticated attack to exploit i.e. they require a man-in-the-middle position between the owners home internet and the Cognitoys servers, these vulnerabilities are nevertheless serious and should be mitigated through employing standard technologies like TLS.

In positive security practices, the Dino companion application does use TLS for communicating with the server and the device itself does require a button being pressed before it will record anything.

This report has been amended in response to comments from the manufacturer.

[7] https://play.google.com/store/apps/details?id=com.majestykapps.cognitoys&hl=en

[8] https://itunes.apple.com/us/app/cognitoys/id1087630536?mt=8

Product Specifications

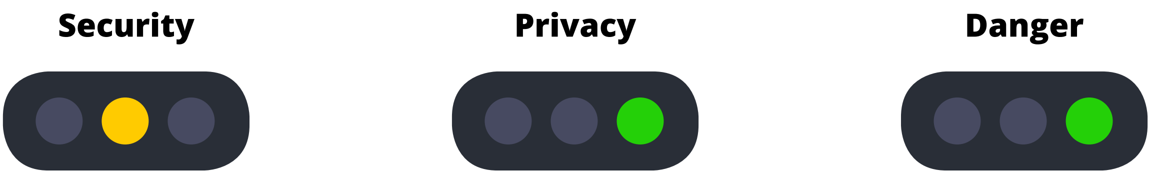
Connectivity	WiFi
Camera	No
Microphone	Yes
Additional Data Collection	The server collects Child Name, Child Play Data and other residual information such as WiFi connection information, IP Addresses etc.

Product Report: BB-8™ App-Enabled Droid™

BB-8 is a Bluetooth-enabled toy that can be controlled via a variety of different applications, the advertised applications with the toy itself are the BB-8 Android[9] and iOS apps[10], but BB-8 will also work with other Sphero enabled applications like Sphero Edu (available on Android[11], iOS[12] and Chrome[13]).

The BB-8 toy itself is light on features, it is possible to control the movement of the device through Bluetooth as well as change the colour of BB-8.

Security Summary



Like most Bluetooth devices on the market BB-8 requires and has no authentication mechanism. While BB-8 can only pair with a single device at a time, once the connection is lost BB-8 becomes available to pair with the next device.

While it is fairly trivial for an attacker to gain control over the BB-8 itself, there is very little that an attacker could accomplish.

In a lab setting we were able to take control over BB-8 and cause the device to act as a strobe at a fast frequency (a standard feature of the Sphero Edu toolkit) - we were also able to use BB-8 sensors to begin to build a map the room - however the practicality and likelihood of such attacks in the real world is questionable.

Per the privacy policy: audio data collected for speech recognition is processed on the device and are not sent to remote servers.

Sphero have an app data deletion process detailed in their privacy policy.

[9] https://play.google.com/store/apps/details?id=com.sphero.bb8&hl=en

[10] https://itunes.apple.com/us/app/bb-8-app-enabled-droid-powered-by-sphero/id1032845453?mt=8

[11] https://play.google.com/store/apps/details?id=com.sphero.sprk&hl=en

[12] https://itunes.apple.com/us/app/sphero-edu/id1017847674?mt=8

[13] https://chrome.google.com/webstore/detail/sphero-edu/hfiocchbmngcelgfdcfbepgoipapddlh?hl=en

Product Specifications

Connectivity	Bluetooth - No Authentication
Camera	No - (App requests camera permission for some features)
Microphone	No - (App requests microphone permission for some features)
Additional Data Collection	App Collects: Age, Location

About

This report was commissioned by Top10VPN.com with all research conducted and authored by Sarah Jamie Lewis.

About Top10VPN.com

Top10VPN.com is the world's largest VPN comparison website. It rates and reviews the best VPN services to help protect consumers' privacy online. The company also aims to educate the general public about the privacy and cybersecurity risks through its free online guides and resources.

About Sarah Jamie Lewis

Sarah is an anonymity and privacy researcher working on projects that help people take control of their own security.

She has worked on preventing fraud through adversarial machine learning, discovering and exploiting weaknesses in telephony and networking protocols and has conducted multiple security assessments of large ecommerce sites and backend systems.

She publishes articles about the security of the Dark Web through mascherari.press - an independent organisation which researches and publishes news articles and technical reports on anonymity, privacy and security in order to help activists, journalists and others protect themselves online and off.