REFERANSE:	DATO:	VERSJON:	ANSVARLIG:
[Skriv inn referanse]	02.11.2016	1.0	Andreas Johnsen

Report

Investigation of privacy and security issues with smart toys

Preface

This report has been written by Bouvet on behalf of the Norwegian Consumer Council. The report is about security and privacy issues regarding smart toys.

Bouvet is a Scandinavian consultancy which works for players in all major sectors who are important for society. Bouvet provide services in information, technology, digital communication and enterprise management and have 1 036 employees at 14 offices in Norway and Sweden.

Summary

Privacy and security regarding smart toys that can talk and interpret speech have been investigated in this report. The three toys that have been tested are Cayla, i-QUE and Hello Barbie. Cayla and i-QUE use similar technology and connects to a user by a phone or tablet while Hello Barbie connects directly to the internet through Wi-Fi.

All of the toys upload recordings of the user to third party servers, and the recordings are encrypted before being uploaded. There is however indications that Cayla and i-QUE might be uploading the recordings to other third parties than it is stated in their user agreements. Cayla and i-QUE can also be connected to by simply searching for nearby Bluetooth devices because they are effectively hands-free headsets, and can be used as recording devices when connected to a phone. This could simply have been fixed by requiring some sort of physical access to be able to connect to the toy, but this has not been implemented. Furthermore, questions to Weather Underground, a weather service, is sent directly by HTTP and are not encrypted, making it easy for a man-in-the-middle to read the data.

Even though Hello Barbie is connected directly though Wi-Fi, making it possible to attack her from anywhere in the world, the microphone is physically connected to a button that needs to be pressed for the doll to be able to record.

Contents

Preface 2

Summary 3

1 Introduction 5

2 Test devices 6
2.1 Toys 6
2.2 Phones/tablets 7

3 What was tested 8
3.1 Internet communication 8
3.2 Bluetooth 8
3.3 Hardware 8

4 Testing setup 9
4.1 Man-in-the-middle 9
4.2 Bluetooth communication 10

5 Findings 11
5.1 Internet Communication 11
5.2 Bluetooth Communication 12
5.2.1 Pairing 12
5.2.2 Range 12
5.2.3 Hardware 14
5.3 Using the toys as recording devices 15
5.4 Findings - iOS 16
5.5 Findings - Android 16

6 App Permissions 18
iPhone (iOS 10) 18
IPhone (iOS 10): Permissions overview 18
Android (5.1.1) 19
Android (5.1.1): Permissions overview 19

1 Introduction

This report concerns itself with the safety of a new generation of toys. These toys are "smart" and can interpret speech, making them capable of having conversations with the child. To enable these new features, the toys are equipped with speakers and microphones, and they can be wirelessly connected to phones/tablets or directly to the internet.

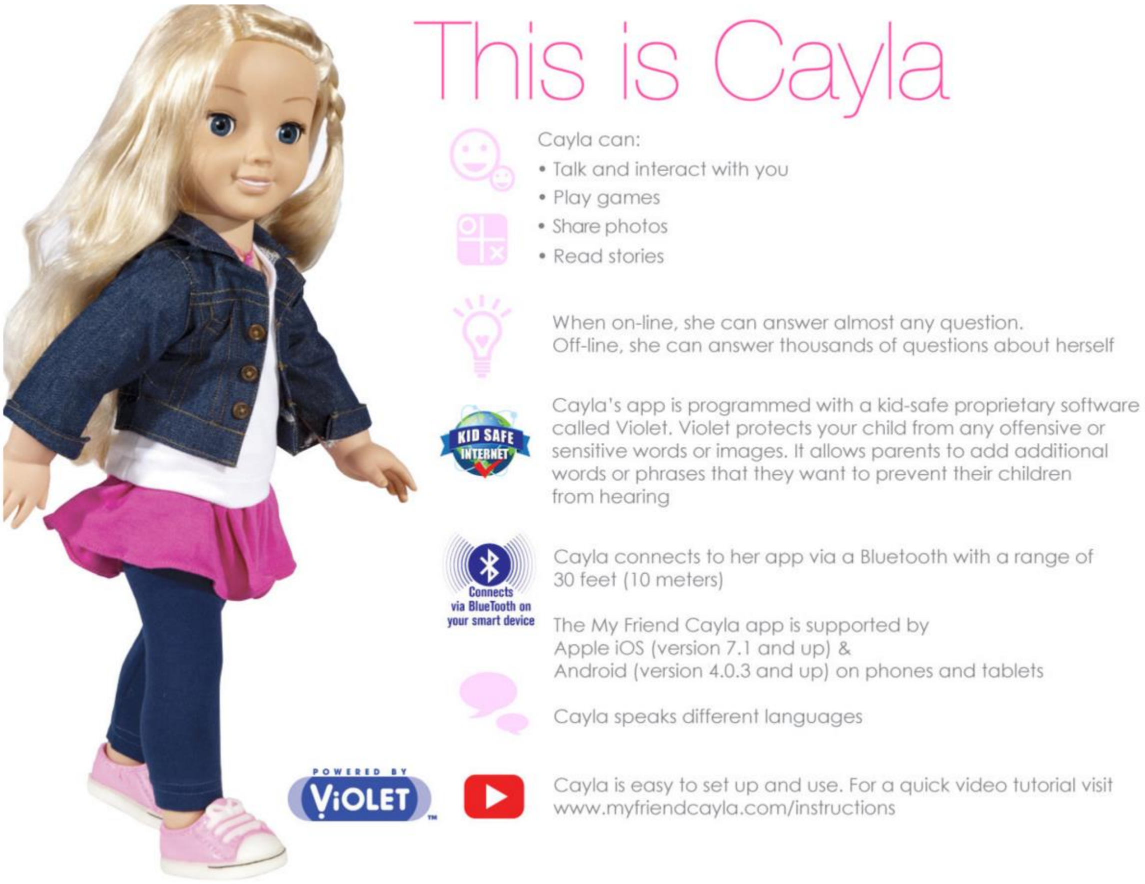
This obviously makes for some safety concerns, as it might be possible for unauthorized people to connect to these toys and use them to monitor the child or home. Furthermore, the toys could potentially be sending information about the usage of the toys to third parties, or be sending information in an insecure matter.

How sensitive information is stored and processed server-side is outside the scope of this report because we do not have access to the manufactures or the third-parties servers. The focus has instead been on what kind of information that is sent, how information is sent and how difficult it would be for an unauthorized user to connect to the toys and use it to gather information.

2 Test devices

2.1 Toys

The three toys that have been tested are Cayla, i-QUE and Hello Barbie.



This is Cayla

Cayla can:

- Talk and interact with you
- Play games
- Share photos
- Read stories

When on-line, she can answer almost any question. Off-line, she can answer thousands of questions about herself

Cayla's app is programmed with a kid-safe proprietary software called Violet. Violet protects your child from any offensive or sensitive words or images. It allows parents to add additional words or phrases that they want to prevent their children from hearing

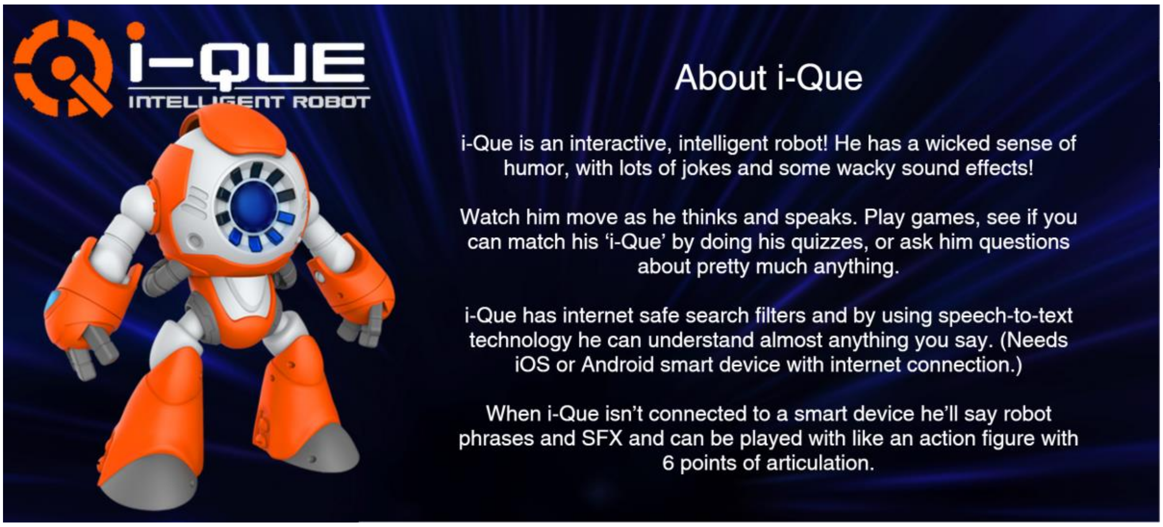
Cayla connects to her app via a Bluetooth with a range of 30 feet (10 meters)

The My Friend Cayla app is supported by Apple iOS (version 7.1 and up) & Android (version 4.0.3 and up) on phones and tablets

Cayla speaks different languages

Cayla is easy to set up and use. For a quick video tutorial visit www.myfriendcayla.com/instructions

Figure 1: Source



About i-Que

i-Que is an interactive, intelligent robot! He has a wicked sense of humor, with lots of jokes and some wacky sound effects!

Watch him move as he thinks and speaks. Play games, see if you can match his 'i-Que' by doing his quizzes, or ask him questions about pretty much anything.

i-Que has internet safe search filters and by using speech-to-text technology he can understand almost anything you say. (Needs iOS or Android smart device with internet connection.)

When i-Que isn't connected to a smart device he'll say robot phrases and SFX and can be played with like an action figure with 6 points of articulation.

Figure 2: Source

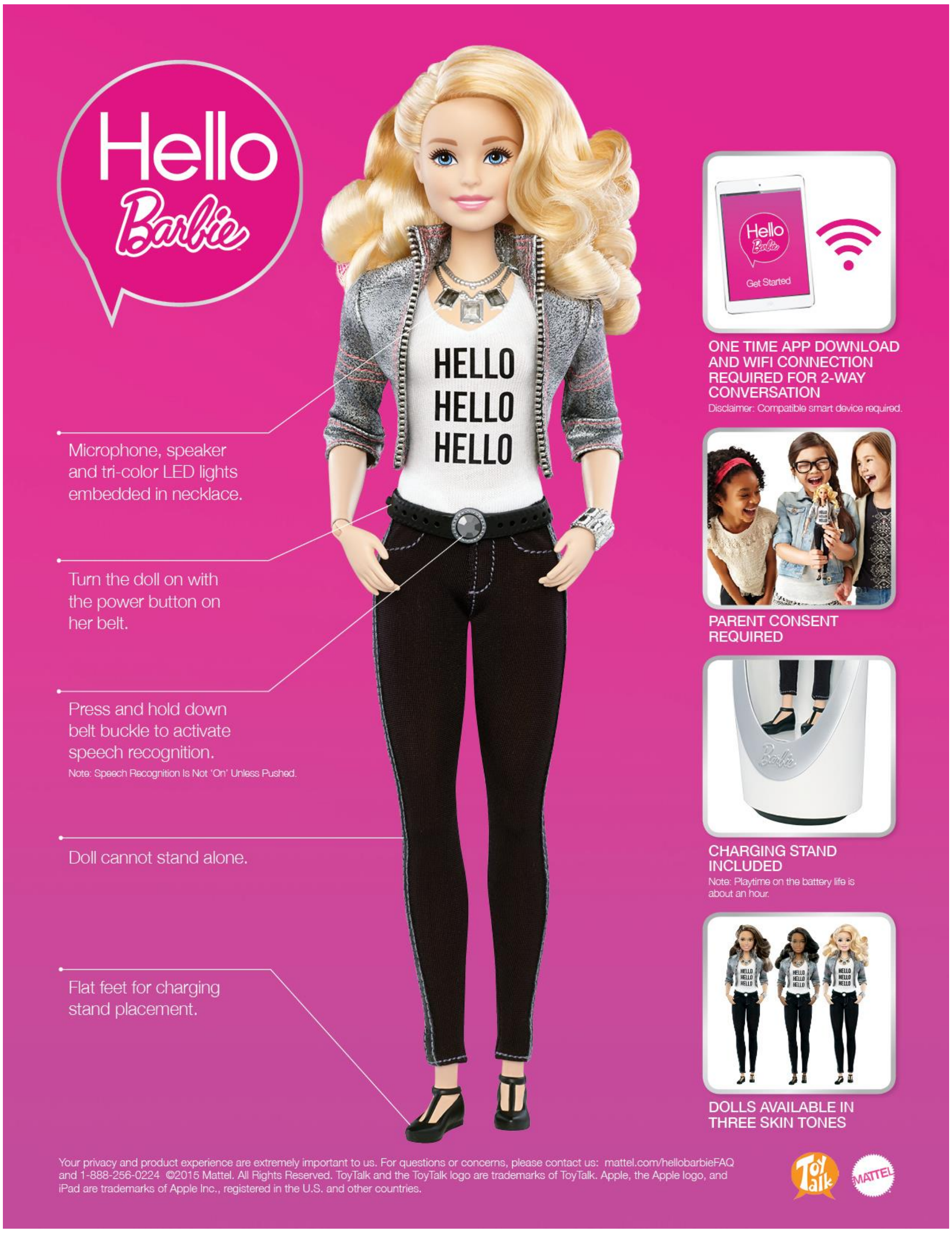

Hello
Barbie
HELLO
HELLO
HELLO
Microphone, speaker and tri-color LED lights embedded in necklace.
Turn the doll on with the power button on her belt.
Press and hold down belt buckle to activate speech recognition.
Note: Speech Recognition Is Not 'On' Unless Pushed.
Doll cannot stand alone.
Flat feet for charging stand placement.
Hello Barbie
Get Started
ONE TIME APP DOWNLOAD AND WIFI CONNECTION REQUIRED FOR 2-WAY CONVERSATION
Disclaimer: Compatible smart device required.
PARENT CONSENT REQUIRED
Barbie
CHARGING STAND INCLUDED
Note: Playtime on the battery life is about an hour.
DOLLS AVAILABLE IN THREE SKIN TONES
Your privacy and product experience are extremely important to us. For questions or concerns, please contact us: mattel.com/hellobarbieFAQ and 1-888-256-0224 ©2015 Mattel. All Rights Reserved. ToyTalk and the ToyTalk logo are trademarks of ToyTalk. Apple, the Apple logo, and iPad are trademarks of Apple Inc., registered in the U.S. and other countries.
ToyTalk
MATTEL

Figure 3: Source

Cayla and i-QUE have a speaker and a microphone inside of them which connects to a phone/tablet by Bluetooth, and they are dependent on the phone/tablet to do the computing. All of the internet traffic from Cayla and i-QUE comes from the phone/tablet that it is connected to. Hello Barbie only needs a phone/tablet during setup; afterwards she is directly connected to the internet through Wi-Fi.

2.2 Phones/tablets

The device used to test the Android apps was a Nexus 4 running Android version 5.1.1 (Lollipop). A Samsung Galaxy S7, running Android version 6.0.1 (Marshmallow) was used during the range test of the Bluetooth communication. An iPad mini (first generation) running version 8.4.1 was used to test iOS devices.

3 What was tested

3.1 Internet communication

The tests were limited to what we considered "normal usage" of the apps and toys. For each app/toy the following tests (if applicable) on both iOS and Android were executed:

- Install the app
- Connect to toy
- Start app / toy
- Adjust settings
- Talking to the toy
- Close app /toy
- Disconnect device

Each app was only tested for a limited amount of time, meaning that the apps could be transmitting more information than we were able to uncover. Our main focus has been encryption and what kind of information that has been sent directly to third parties.

3.2 Bluetooth

Cayla and i-QUE use Bluetooth to communicate with the smart phone or tablet it is connected to. Hello Barbie on the other hand connects to the phone/tablet by setting up a temporary Wi-Fi network, and do not use Bluetooth at all.

The safety of the Bluetooth communication between the toys and the phones/tablets have not been tested, instead the focus have been on the pairing process between the devices and the range of the communication. Standard Bluetooth communication is largely considered safe once a connection has been established, unlike Bluetooth low energy (BLE) which are not used by these toys.

For each toy, the following tests (if applicable) were executed:

- Connecting to the toy
    - When the phone and toy had not been connected before
    - When the phone and toy had been connected before
- Disconnecting from the toy

Most of the tests have been executed inside, except for some range tests, which were partially outside. The range tests were used to test the range of which it is possible to connect to Cayla and i-QUE. Three different test scenarios was used:

1) Range of communication in an open space
2) Range of communication when there is a window in between the phone/tablet and the toy
3) Range of communication where there is a concrete wall between the phone/tablet and the toy

The tests were executed by using regular phones/tablets, i.e. no special equipment. It is important to note that more powerful transmitters/receivers are available, though this has not been tested.

3.3 Hardware

Cayla and Hello Barbie was opened up so that we could see what kind of hardware was hiding inside of them. This was to look for hardware vulnerabilities and to determine what kind of security the hardware could support.

4 Testing setup

4.1 Man-in-the-middle

To monitor the communication between the app and its web-services a man-in-the-middle approach was taken. This was achieved by routing all of the Internet traffic between the phone/tablets through our computer, making it what is known as a proxy-server. This made it possible to see what information was transmitted between the app and the various Internet servers and how often the communication occurred. Fiddler[1] was used to monitor the Internet Traffic and to create the proxy server.

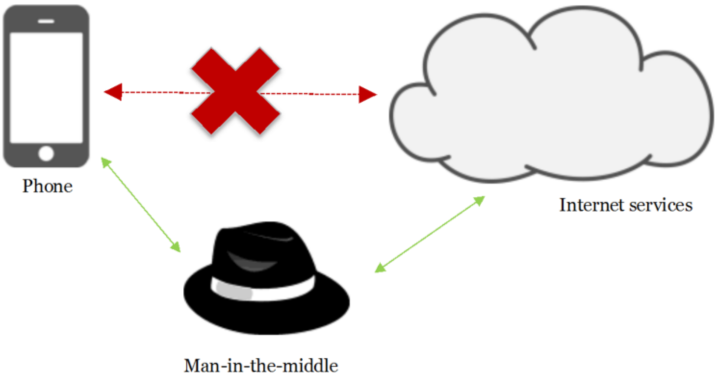
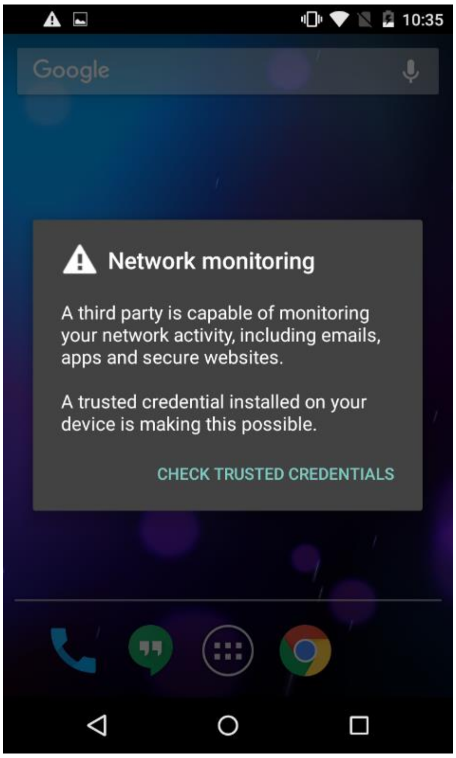


Figure 4: Overview of a man-in-the-middle attack

All of the apps uses SSL encryption on most of the Internet traffic. This is an added security layer to the unsecure HTTP message protocol, and is known as HTTPS. To break this encryption a custom root-certificate, provided by Fiddler, was installed on the phones/tablets. A root-certificate tells the phone which servers it can trust on the Internet, and the certificate provided by Fiddler makes the phones/tablets trust our proxy-server, enabling us to decrypt the traffic. This is not regarded as a security flaw as 1) it requires physical access to the phone/tablet and the knowledge of how to unlock it, and 2) the phone/tablet displays a big warning notification about being unsecure when a custom root-certificate is installed, see Figure 5.

Hello Barbie also uses SSL. However, it is very difficult to install a root-certificate and configure the toy for our proxy server, if even possible. With the other toys the root certificate is installed on the phone, but this is not possible on Hello Barbie as it talks directly to the Wi-Fi. The best we could do in terms of monitoring the internet traffic was to route the traffic through our man-in-the-middle without decrypting the messages. Even though the content of the messages are hidden it is possible to see which message protocols are used and which IP addresses the data is being sent to. Wireshark[2] was used to look at the messages.



Network monitoring

A third party is capable of monitoring your network activity, including emails, apps and secure websites.

A trusted credential installed on your device is making this possible.

Figure 5: Screen shot of phone with a custom root-certificate installed

[1] More information about Fiddler
[2] More information about Wireshark

4.2 Bluetooth communication

The concrete wall used in the test was about 20cm thick and the windows where double-pane. The range tests were executed using a galaxy S7, and both Cayla and i-QUE were tested separately. New batteries were inserted into the toys before the tests.

Sound quality is hard to define, but the toys were placed next to a person that was talking, and then we tried to find the maximum distance between the phone and the toy before it became difficult to understand what the person was saying when using the toy as a recording device.

To test the range of the pairing between the phone/tablet and the toys we started with a good distance between the two and moved the two closer and closer together until they were able to pair. This was repeated three times for each test to ensure a good result.

5 Findings

5.1 Internet Communication

All the apps use HTTPS (encryption) when utilizing network communication, except for Cayla and i-QUE when talking to Weather Underground (more on this later). When asking questions to Cayla and i-QUE the speech-to-text functions is handled by the app, compared to Hello Barbie that sends a file containing the recording directly to toytalks servers for interpretation. However, we did find that Cayla and i-QUE (both on iOS and android) uploaded data to the IP address 205.197.192.116. This data was sent while recording, and the size of the data indicates that it was sound files.

In the agreements[2,3] for Cayla and i-QUE it states that "When you ask the app a question, this information request is stored on a Nuance Communication (for Apple-based users) or IVONA or Google (for Android/Google-based users) server in the cloud." On Android the apps sends a request to the nuance.com[5] webpage when they launches. If the apps cannot get the website they tell the user that they cannot connect to the internet, so the apps might use it as a test to see if they have access to Internet. The IP address 205.197.192.116, which is the IP address the apps uploads what we believe to be recordings to, is from Massachusetts Burlington, which is the same city where Nuance has their main offices.

Furthermore, in the agreements[3,4] it also states that the toys use the following search engines to answer questions: Google search, Wikipedia and Weather Underground[5]. In our tests we were able to observe questions going to Wikipedia and Weather Underground, but we did not find any google searches. This could be because we were not able to ask the right trigger questions, or because the Norwegian app does not use google. The questions that are sent to Weather Underground are sent over plain HTTP and are not secure, making it very easy for a man-in-the-middle attack to pick up this data. The agreements[2,3] also includes that "ToyQuest and/or its Licensors may collect and use the contact names that appear in your address book", but we did not observe the address book being sent to the manufacturer or third party servers.

We were not able to see the calls to the IP address 205.197.192.116 and to Weather Underground using our proxy server, but we were able to see them in Wireshark when connecting the phone/tablet to a Wi-Fi hotspot setup from our PC. It is unclear how the traffic was able to circumvent the proxy setup on our phone/tablet, but in the end it makes no real difference in terms of security.

When first starting up the Hello Barbie Companion app it notifies stats.unity3d.com about the hardware of the device, including a universally unique identifier. How this identifier is created is unknown, but it is most likely connected to the device. When starting up the app the parent is asked to create an account on Toytalk.com and is required to enter an email address and create a password. The parent can then log into the website and listen to or delete the recordings made by the doll. It is possible to delete the account on Toytalk.com and we found that it was possible to recreate the account with the same email, but then all of the old recordings were gone.

In our investigation of the data sent from Hello Barbie we found that messages were being sent to two IP addresses: 162.125.18.133 and 162.125.34.129. Both are from San Francisco (California) where Toy Talk offices are located. We found that the connection uses SSL, meaning that the connection is secure. It seemed like the two IP addresses were in use when Hello Barbie answered a question or when uploading a recording. We can not know for sure what Hello Barbie uploads as we can not decrypt the traffic, but by looking at when data was sent to these IP addresses and when the recordings showed up on Toytalk.com we deduced that the recordings were included in these messages.

[3] http://myfriendcayla.co.uk/agreement
[4] http://ique-robot.co.uk/user-agreement
[5] wundergroud.com

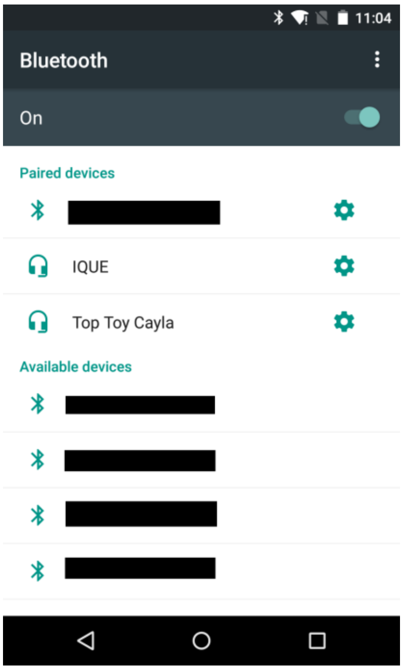
Hello Barbie was smart enough to be able to answer questions like “what is your name”. However, when Hello Barbie asked the user a question like “What is your favorite color” it did not always matter what the user answered, she would maybe say “cool, that is a nice color!” or a similar generic answer.

5.2 Bluetooth Communication

5.2.1 Pairing

Cayla and i-QUE use no security measures when pairing to the phone/tablet. As long as the toys are turned on, and not connected to another device, they can be found and connected to by other Bluetooth devices. We also tested if the toys were discoverable only during a short time span after being turned on, but leaving the toys on for 30 minutes showed that they were still discoverable. Their names when searching for Bluetooth devices are "Top Toy Cayla" and "IQUE", making them easily recognizable (see Figure 6). The phones/tablets thinks the toys are hands-free headsets, so no apps are needed to connect to the toys. The toys have no indicators of being connected to a device, but Caylas necklace and i-QUEs eye lights up when the microphone is turned on.

This could easily be fixed by having a method of ensuring that a person has physical access to the toy before being able to connect. This could be a physical button on the toy that needs to be pressed during paring with a new device, or an even safer approach would be to require the user to enter a random generated passkey when pairing with a new device, ensuring that the physical button on the toy is not accidently pressed. Which option to implement (or not any at all) is most likely a trade off between cost/usability and security, see section 5.2.3. Currently it is possible to stand outside a building and connect to the device given that it is within range, turned on and not connected to another device.



Bluetooth

On

Paired devices

[redacted]

IQUE

Top Toy Cayla

Available devices

[redacted]

[redacted]

[redacted]

[redacted]

Figure 6, Screenshot on Android during pairing process

5.2.2 Range

5.2.2.1 Open space

In the first test the range of the communication was tested in an open space. In Figure 7, the picture is taken from the perspective of the person holding the phone. The producer of the toys states that the Bluetooth communication has a range of 10 meters[6]. In our testing, the distance could not be more than 13 meters when connecting to the toys for the first time. If however the phone had been connected to toys at an earlier time the distance were 20 meters. At this distance it was also possible to record sound without any major reduction in sound quality.

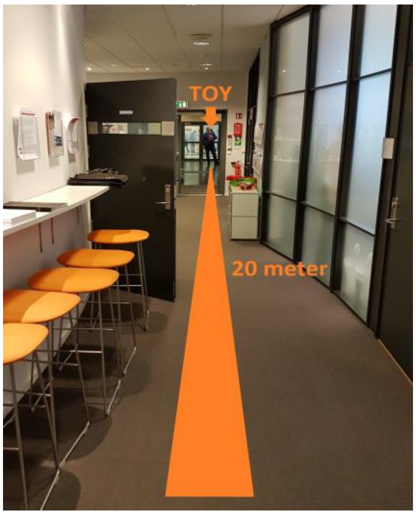


Figure 7

[6] iOS Cayla Video Instructions

5.2.2.2 Window (double-pane)

In this test the range of communication was tested outside the building and through a double pane window. Connecting and making recordings through the double pane window was more difficult than through open air. If the phone had never connected to the toy before the distance needed to connect was roughly 1 meter. If the phone had been connected to the toy at an earlier time it was possible to connect to the toy from 5 meters. After having connected to the toy we found that it was possible to understand what the other person was saying even when the phone was 10 meters away from the window (Figure 8/9).

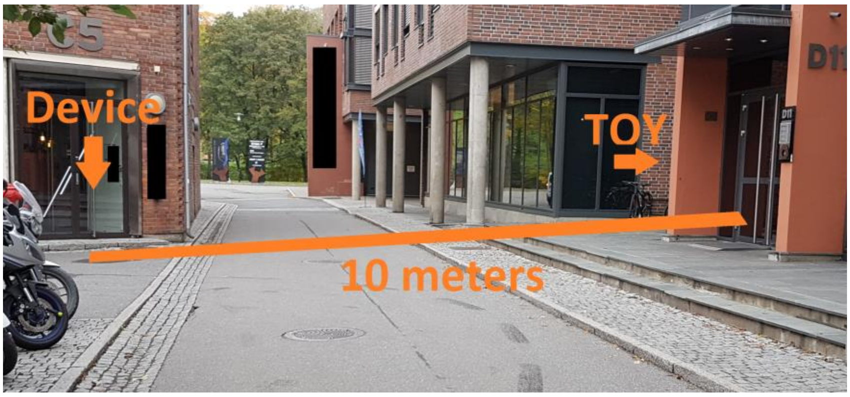


Figure 8

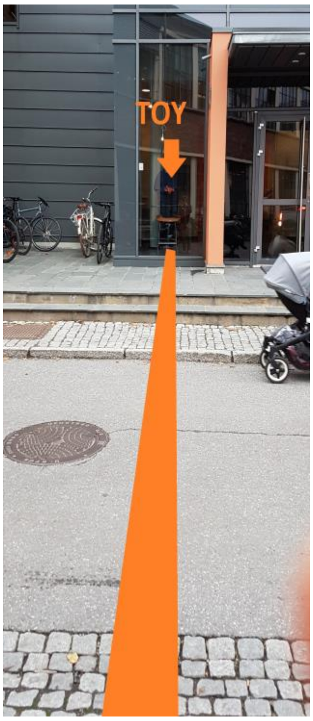


Figure 9

5.2.2.3 Concrete

Instead of showing a picture of the test scenario, a drawing of the floor plan and the placement of the phone and toy has been made, see Figure 10. The toys were placed in the stairway while the person with the phone went into a nearby toilet stall. During this test we were not able to discover or connect to the toys when the toys had not previously been connected to the phone. However, when the toys had been discovered by the phone earlier it had no problem connecting. Furthermore, sound quality was good and it was easy to hear what the other person was saying.

While this test were meant to showcase how the Bluetooth signal would degrade because of the concrete wall, it was difficult to ensure that the signal was really going through the wall. As can be seen in Figure 10, it is a possibility that the signal was going around the wall instead, but this was the closest scenario we were able to achieve in our offices.

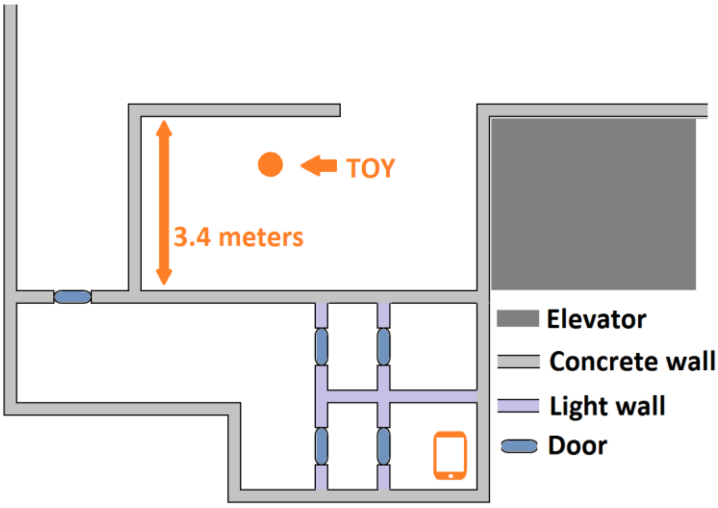


Figure 10, Rough sketch of floor plan

5.2.3 Hardware

We opened up Cayla to see what the kind of technology that was hidden inside of her. What we found was a custom circuit card with a Bluetooth module based on chip IS1685S from ISSC. The Bluetooth standard supports several task flows for pairing devices with different security levels. The Bluetooth module in Cayla supports Bluetooth 2.1 Secure Simple Pairing. Secure Simple Paring supports the "Just Works" task flow which requires no user actions. This task flow is "…useful whenever product implementers want to make the user experience easier and have accepted the increased risk of security attacks." [7]

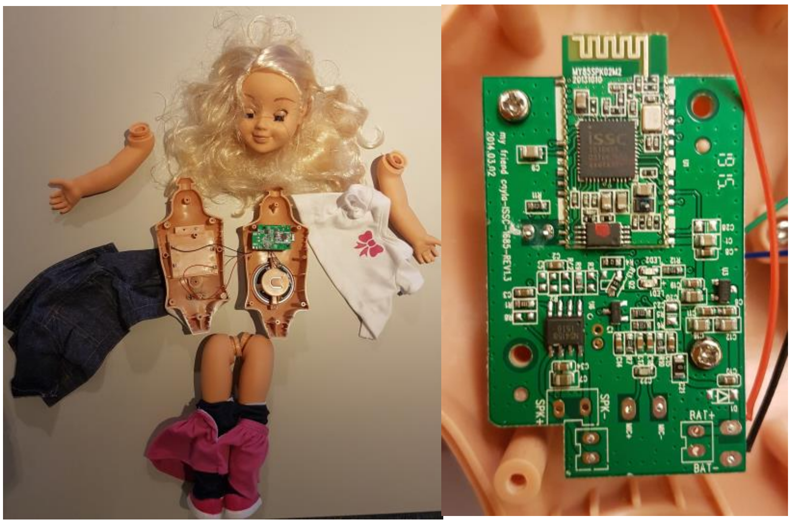
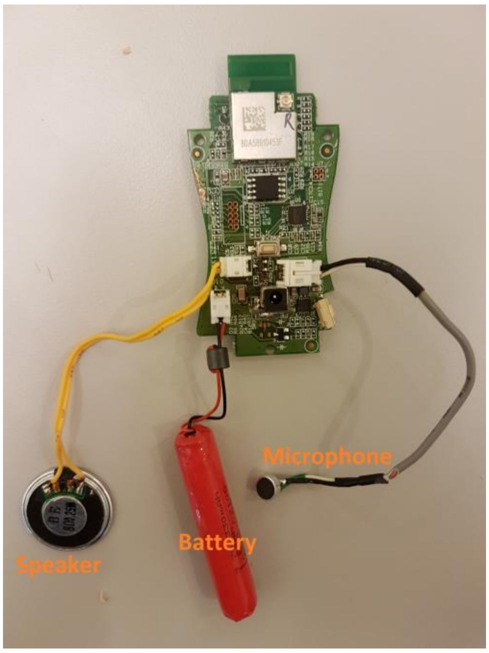


Figure 11, Cayla opend up

We also opened up Barbie. To make a recording using Barbie the user has to press a button on her belt. The main goal of opening her up was to determine if the microphone and the button were physically connected or just by software. Multiple parts on the PCB were not labeled so we were not able to determine this by looking at the PCB. However, by measuring the voltage difference between the button and the microphone revealed that there was a voltage difference of 1V when the button was not pressed, but that the difference disappeared when pressing the button. From this it seems very likely that the button and the microphone are physically connected in such a manner that it is impossible to use the microphone if the button is not pressed.



Figur 12, Barbie opend up

[7] Bluetooth® User Interface Flow Diagrams for Bluetooth Secure Simple Pairing Devices, Usability Expert Group

5.3 Using the toys as recording devices

Caylas necklace and i-QUEs eye light up when the microphone is turned on, and this would be the only way to know if someone were using the toys unauthorized. By using free apps on the Android playstore we found it possible to use Cayla and i-QUE as recording devices, and by calling the phone that is connected to the toy it is possible to achieve two-way communication with the toy by using it as a hands-free headset. This is very easy and requires little technical know-how! Presumably, it would not be too difficult to make an app to enable two-way communication using a single phone, though we were not able to find such an app on either Android or iPhone in the app/play-store.

By comparison, Babies necklace lights up when she is turned on, and the lights blinks in different colors and patterns depending on her state. When she records the light to her right has a steady green color, though this is done through software. However, it is necessary to press and hold a button on Hello Barbie to be able to use the microphone, and it seems to be a hardware connection (see previous section). If it was only software then a hacker could potentially use Barbie as a recording device by circumventing the software (assuming the hacker was able to gain full control over the doll), but this is not the case.

While it is a lot easier to connect to Cayla and i-QUE it requires the "hacker" to be within close range. Barbie on the other hand is exposed to the internet, meaning that she can be attacked by anyone in the world. While we were not able to find any loopholes such that we could connect to her and read her data it is possible that security vulnerabilities can be found in the future, and Hello Barbies software will not be patched forever. However, no software attack will ever be able to make the microphone work without the button on her belt being pressed.

5.4 Findings - iOS

Name of toy	Cayla	i-QUE	Hello Barbie
Name of app / version	My firend Cayla (Norsk)/2.0.1	i-QUE Robot App (Norsk)/1.0.1	Hello Barbie Companion App/1.6
Man-in-the-middle attack	Yes	Yes	No*
Secure communication	SSL/HTTP	SSL/HTTP	SSL*
Manufacturer servers	IP: 205.197.192.116[5]	IP: 205.197.192.116[5]	Api.2.toytalk.com*
Third party servers	No.m.wikipedia.org[2] api/wunderground.com[4]	No.m.wikipedia.org[2] api/wunderground.com[4]	Stats.unity3d.com
Transmits data to Facebook	No	No	No
Trackers/Adware	No	No	No
Application transmits data in the background	No	No	No

*When turning on the Hello Barbie Companion App there are many attempts to connect to Api.2.toytalk but Fiddler throws an error that something went wrong during the SSL handshake. It is not possible to log into the application when the man-in-the-middle attack is used. It is unclear why, but it might be that a technique similar to SSL pinning is being used.

5.5 Findings - Android

Name of toy	Cayla	i-QUE	Hello Barbie
Name of app / version	My firend Cayla (Norsk)/2.0.1	i-QUE Robot App (Norsk)/1.0.1	Hello Barbie Companion App/1.3
Man-in-the-middle	Yes	Yes	Yes
Secure communication	SSL/HTTP	SSL/HTTP	SSL
Manufacturer server	IP: 205.197.192.116[5]	IP: 205.197.192.116[5]	Api.2.toytalk.com

Third party server	www.nuance.com[1] No.m.wikipedia.org2 api/wunderground.com[4]	www.nuance.com[1] No.m.wikipedia.org2 api/wunderground.com[4]	Stats.unity3d.com
Transmits data to Facebook	No	No	No
Trackers/Adware	No	No	No
Application transmits data in the background	No	No	No

[1]**www.nuance.com**: From myfriendcayla.co.uk/agreement: "When you ask the App a question, this information request is stored on a Nuance Communication (for Apple-based users) or IVONA or Google (for Android/Google-based users) server in the cloud." We found no indication of the app talking to IVONA.

[2]**no.m.wikipedia.org:** When asking a question to either i-QUE or Cayla the interpreted text is sent as a search to the Wikipedia API. No user sensitive information was found.

[3]**stats.unity3d.com:** Unity3d is a tool to create applications. The data sent contains information about the hardware of the device, such as model, OS, screen size etc, but also a universally unique identifier. The data is only sent when opening the app for the first time after installation.

[4]**api/wunderground.com:** This is a weather service used by Cayla and i-QUE. The request is made using HTTP, and a man-in-the-middle can very easily see the messages. The request messages are rather cryptic, but the return answer is pretty easy to read. Click here for an example for a request for the weather in Oslo.

[5]**IP address: 205.197.192.116:** When Cayla and i-QUE are recording, on both android and iOS, they are sending data to this IP address. During 6.3 seconds of recording roughly 10.2kb are sent. This translates to a bit rate of about 12kbps. Compared to a normal mp3 with a bit rate of 128kbps this might seem very small, but the human voice has a much narrower voice frequency band compared to what we are need when listing to music. Furthermore, this is just a mono recording (one microphone). Because of this it is possible to store the audio much more efficiently, and 12kbps is enough to transfer audio of human voice[8].

[8] AMR-NB decoder

6 App Permissions

iPhone (iOS 10)

Name of toy	Cayla	i-QUE	Hello Barbie
Name of app/version	My firend Cayla (Norsk)/2.0.1	i-QUE Robot App (Norsk)/1.0.1	Hello Barbie Companion App/1.6
Microphone	Yes	Yes	No
Bluetooth	Yes	Yes	No

IPhone (iOS 10): Permissions overview

Microphone: Gives the application access to the microphone.

Bluetooth: In Norwegian: “Slå på Bluetooth for å tillate at <app name> kobler seg til Tilbehør”. Translated into English: “Turn on Bluetooth to allow <app name> to connect to devices”

Android (5.1.1)

Name of toy	Cayla	i-QUE	Hello Barbie
Name of app/version	My firend Cayla (Norsk)/2.0.1	i-QUE Robot App (Norsk)/1.0.1	Hello Barbie Companion App/1.3
Wi-Fi connection information	Yes	Yes	No
Photos/Media/Files	Yes	Yes	No
Microphone	Yes	Yes	No
Bluetooth connection information	Yes	Yes	No
Storage	No	No	Yes
Network communication	No	No	Yes

Android (5.1.1): Permissions overview

Wi-Fi connection information: “Allows the app to view information about Wi-Fi networking, such as whether Wi-Fi is enabled and names of connected Wi-Fi devices”.

Photos/Media/Files: “Uses one or more of: files on the device, such as images, videos, or audio; the device’s external storage”.

Microphone: “Uses the device's microphone(s)”.

Bluetooth connection information: “Allows the app to control Bluetooth, including broadcasting to or getting information about nearby Bluetooth”.

Storage: “Allows the app to write to the USB storage”.

Network communication: “Allows the app to connect to and disconnect from Wi-Fi access point and to make changed to device configuration for Wi-Fi networks”.