



Hello Barbie



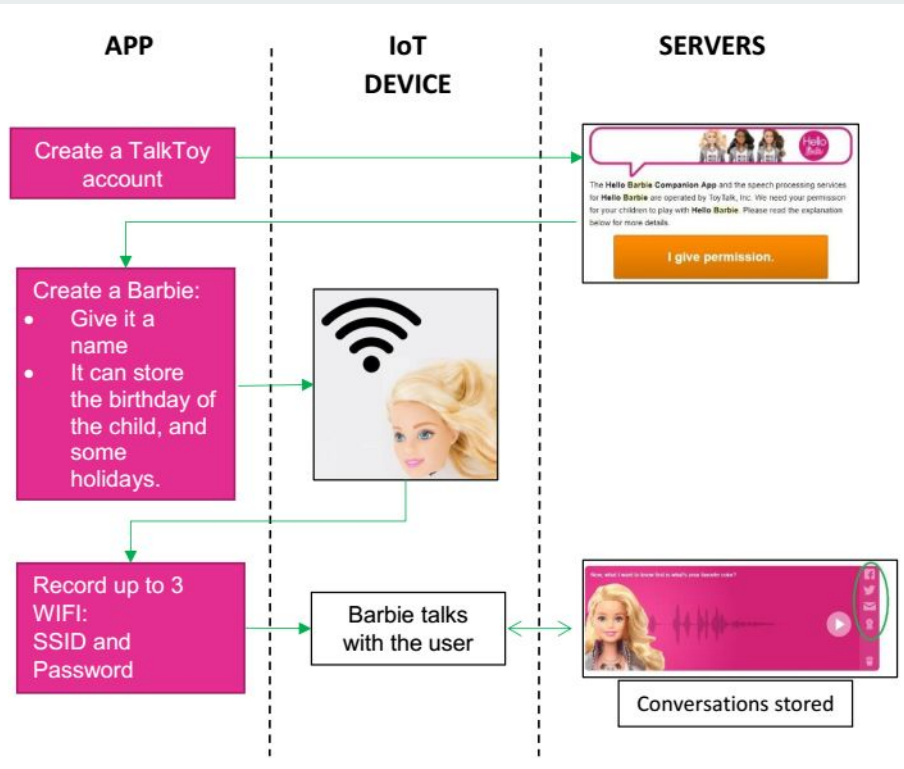
Lucia Botiquin
Kavya Kurup
Zeqing Li
Matthew Valencia





How does it work?

Initial configuration:



Account belongs to parent, requires they give permission for their child to use doll.

The user interacts with the device in an iterative two step process. First, the Barbie ask something, and second the users says the answer, they press a button to start recording audio and release the button to stop.

The recording is transmitted through wifi to a server, stored, and processed to determine an appropriate auditory response. Wifi credentials stored "encrypted" in device. Physical reset button to "forget" all stored credentials.

Note buttons to share recording on social media and to share through email.



Privacy Policy

About Privacy

Hello Barbie™ is not always on. You have to hold down her belt buckle button to activate speech recognition.

Parental consent is required to set up a parent account and connect with Hello Barbie™.

Should parents choose to, all recorded conversations can be deleted at any time.

There is no advertising content within Hello Barbie™.

Your children's conversations are not used to advertise to your child.

OK

Email Messaging

☒ Content update notifications

☒ Mandatory service announcements

Update preferences

+ Web beacon technology

Thank you for your permission to allow your child to use **Hello Barbie™!**



Hello Barbie involves the recording of audio. We use these recordings so your children can talk with **Hello Barbie**. We also use these recordings to share the great stuff your children create with you, to test and improve our services and technologies in areas like speech recognition, and for other research and development and data analysis purposes. We do not use these recordings or their content to contact children or to advertise to them. For more details about our privacy practices with respect to children, please read our [privacy policy](#).

The permission we received from you allows us to collect, use or disclose this information as described in our children's privacy policy. This permission applies to all **Hello Barbie** dolls that are added to your ToyTalk account. Nothing is shared to Facebook, Twitter, or any other social media sites unless you, the parent, choose to do so.

If you would like to withdraw your permission, please click [here](#).

Revoke Permission

Please note that it may take up to 5 minutes for any open ToyTalk apps to detect that you've revoked your permission. After this time, your children will not be able to talk with any ToyTalk apps.

Revoke Permission

Cancel

Parent may delete recordings, but ... “We may periodically delete voice recordings from your parent account, but in such case, we may still have access to those voice recordings for research and development purposes.”

Are you really sure you want to delete your account? There is no way back!

Current Password

Delete Account

Cancel

Claims they may share data “during negotiations of, any merger, sale ... or in any other situation where personal information may be disclosed or transferred as one of the business assets of ToyTalk.”

OWASP ZAP

- ▼ Alerts (9)
 - ▶ X-Frame-Options Header Not Set (4)
 - ▶ Cookie No HttpOnly Flag (5)
 - ▶ Cookie Without Secure Flag (2)
 - ▶ Cross-Domain JavaScript Source File Inclusion (6)
 - ▶ Incomplete or No Cache-control and Pragma HTTP Header Set (34)
 - ▶ Password Autocomplete in Browser (2)
 - ▶ Private IP Disclosure
 - ▶ Web Browser XSS Protection Not Enabled (2)
 - ▶ X-Content-Type-Options Header Missing (65)

- ▶ <https://www.kidsafeseal.com>
- ▶ <https://www.youtube.com>
- ▶ <https://ssl.google-analytics.com>
- ▶ <https://toytalk.com>
- ▶ <https://raw.githubusercontent.com>
- ▶ <https://www.gstatic.com>



Almost all the vulnerabilities were due to third-party plugins that were included on the website (Google, Twitter, and Facebook).

If you choose to use a widget, ToyTalk abstains from the legal responsibility of the privacy of the data shared with a third party.

The liability of the user's browser deems a major reason for the possibility of an attack.

Many of the alerts contained Youtube's url, however, Youtube was not found on the website.

NMAP

```
nmap -A -v -Pn 192.168.0.16
```

Host is up (0.0052s latency).
All 1000 scanned ports on 192.168.0.16 are closed
MAC Address: 28:C2:DD:FF:9F:08 (AzureWave Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: 2N Helios IP VoIP doorbell (95%), Advanced Illumination DCS-100E lighting controller (95%), AudioControl D3400 network amplifier (95%), British Gas GS-Z3 data logger (95%), Daysequerra M4.2SI radio (95%), Denver Electronics AC-5000W MK2 camera (95%), DTE Energy Bridge (1wIP stack) (95%), Enlogic PDU (FreeRTOS/1wIP) (95%), Espressif esp8266 firmware (1wIP stack) (95%), Espressif ESP8266 WiFi system-on-a-chip (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 5.17 ms 192.168.0.16

NSE: Script Post-scanning.
Initiating NSE at 13:12
Completed NSE at 13:12, 0.00s elapsed
Initiating NSE at 13:12
Completed NSE at 13:12, 0.01s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.
Nmap done: 1 IP address (1 host up) scanned in 24.24 seconds
Raw packets sent: 1081 (50.366KB) | Rcvd: 1321 (53.876KB)

The device communicates with server via WiFi, so we do a nmap scan with -A option on it.

-A: Enable OS detection, version detection, script scanning, and traceroute

-Pn: Treat all hosts as online -- skip host discovery.

Wireshark

The image shows the Wireshark network protocol analyzer interface. The main window displays a list of captured packets on the left, with packet 7 selected. The packet details pane on the right shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane at the bottom shows the raw data of the selected packet. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The top toolbar contains various icons for file operations, capture control, and analysis tools.

hellobarbie.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 1

Wireshark · Follow TCP Stream (tcp.stream eq 1) · hellobarbie

No.	Time	Source
5	12.924606	19
6	12.927619	19
7	12.930466	19
8	12.976918	52
9	12.976921	52
10	12.976980	52
11	12.978915	19
12	13.028416	52
13	13.051621	19
14	13.054373	19
15	13.054780	19
16	13.100122	52
17	13.100124	52
18	13.101783	19

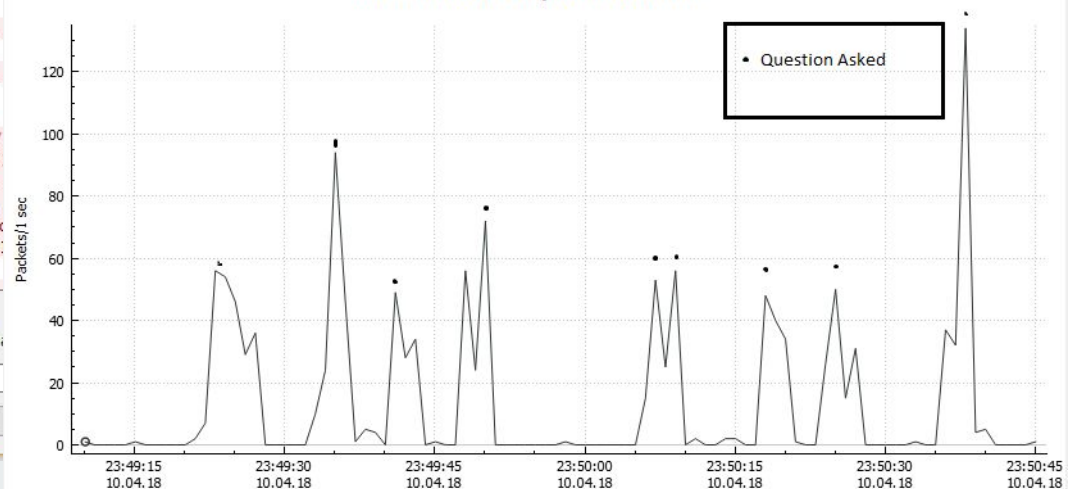
Frame 7: 1514 bytes
Ethernet II, Src: Az
Internet Protocol Ve
Transmission Control

398 client pkts, 82 server pkts, 107 turns.
Entire conversation (429 kB) Show and save data
Find:
Filter Out This Stream Print Save as... Back

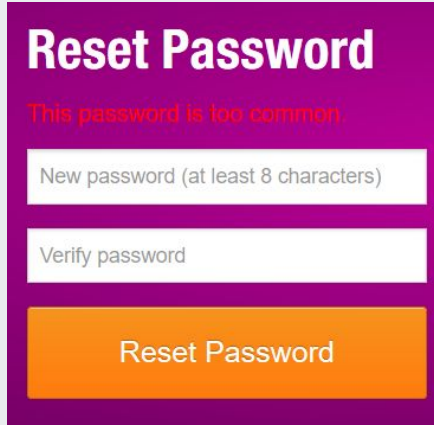
Conversations with cloud server is encrypted over SSL/TLS 1.2

This pattern might not seem to be a privacy vulnerability as long as the content is encrypted. However, the traffic pattern overtime can be a valuable information for unwanted advertisements.

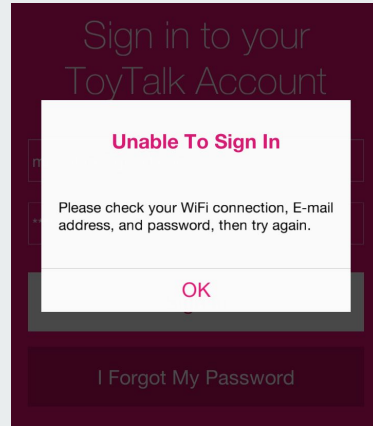
Wireshark IO Graphs: hellobarbie



Password



A purple rectangular form with a white header area. At the top, it says "Reset Password" in large white letters. Below this, in red text, it says "This password is too common". There are two white input fields: the first is labeled "New password (at least 8 characters)" and the second is labeled "Verify password". At the bottom is a large orange button with the text "Reset Password" in white.



A dark purple rectangular form. At the top, it says "Sign in to your ToyTalk Account" in white. In the center, there is a white box with a pink border. Inside this box, it says "Unable To Sign In" in pink, followed by "Please check your WiFi connection, E-mail address, and password, then try again." in black. Below this box is a pink "OK" button. At the bottom of the form is a link that says "I Forgot My Password" in white.

Password Characteristics -
Minimum 8 characters
No required charset
Spaces allowed
Simple dictionary check enforced.

Forgotten Password-
Must reset through an email link, which expires after one day or one use.

No password attempt limitation.
Brute Forceable!

