IoT for Kids: Cayla Doll Exploit

Cheryl Torano

Abertay University

Abstract

This project used only open sourced software to successfully exploit all four levels of the Cayla Doll App's built in safety features.

To achieve this, a technique known as reverse engineering was used. It involved, editing the contents of the Cayla Doll APK file, digitally signing it and then re-compiling it back to APK format, using a tool which can decode resources to nearly original format and then rebuild them again.

This edited Cayla Doll APK, was then installed on an Android Device, and successfully used in conjunction with the Cayla Doll.

Proving that a toy which is designed for children can be easily transformed from a sweet innocent Doll, into a foul mouthed nightmare.

Introduction

Cayla is an Interactive Talking Doll that is designed for children [1]. The Doll connects to a Smart Device via Bluetooth, and can be controlled by the Cayla Doll Application. The App has built in security features, to stop the Cayla Doll from saying inappropriate things or search for unsuitable content on the Internet.

***Figure 1**: Cayla Doll*

The Application, when paired with the Doll, can answer questions, understand and chat, tell stories & play games.

Cayla's App comes with different games that the child can play either with Cayla or against Cayla. She will work offline however, Cayla can only use all of her play capabilities if she's connected to a smart device via Bluetooth. The App can be downloaded, free of charge and is compatible with iOS and Android devices.

The main aim of this project was to bypass the App's built in security features and access Cayla's Database of questions & "bad words" with the intention of editing it, to allow the Cayla Doll to say inappropriate words.

Methodology

Download APK: The Cayla Doll APK was downloaded and the contents extracted.

***Figure 2**: Cayla Doll App's main screen **BEFORE** changes were made.*

Edit files: Due to the lack of security within the APK file, all contents were easily extracted (figure 3) using WinRAR software.

This serious lack of encryption allowed for several changes to be easily made.

All pre-installed story text was edited using Notepad text editing software.

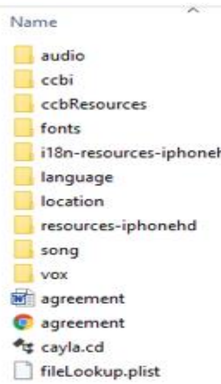

***Figure 3** – Contents of Cayla Doll's APK file.*

Image/audio files were replaced with files sourced from the Internet. Changes were also made to the App's main screen using a free trial of Photoshop software.

The App's SQL Database was viewed using a universal database tool named DBeaver [2]. Which allowed for the blocked word table to be not only viewed but also removed completely.

Recompile the APK: After editing, the file was digitally signed using APK Sign software then recompiled using APKTool [3], which is a tool for reverse engineering 3rd party, closed, binary Android apps. It can decode resources to nearly original format and then rebuild them, ready to be installed & used on any Android Device.

Results

Install APK: The edited APK was then installed & used in conjunction with the Doll.

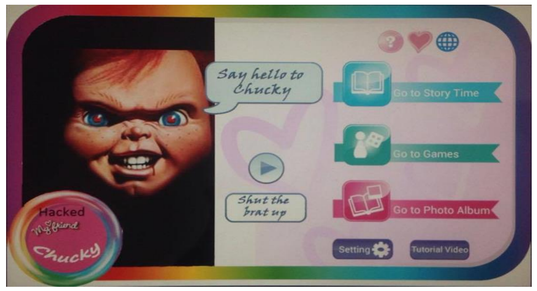

***Figure 4**: Cayla Doll App's main screen **AFTER** changes were made.*

The Cayla Doll Application uses specially designed Voice Operative Learning & Entertainment Technology (ViOLET) which has four levels of security, to scan for inappropriate content. The ViOLET software system, not only checks for any offensive or sensitive words against a pre-set blocked word list, but also uses the same blocked word list for its online safe-search filters, which scans responses for inappropriate content. Therefore, if the Doll is asked a question which contains any words on the blocked word list, or tries to search for inappropriate content on the Internet, Cayla will automatically tell the child she cannot talk about those things.

By deleting the badword table, it allowed for the once sweet & innocent Cayla Doll to now say inappropriate words and access internet content that is not suitable for children.

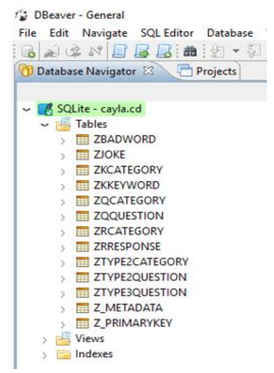

Figure 5 – Contents of Cayla Doll App's SQL Database

Conclusion

There is no password to protect the connection, therefore access to the doll is completely unsecured. Significant extra safety features, including advanced APK encryption needs to be implemented in the Doll before it is safe for children to use.

Countermeasures

Currently when the App is asked a question, this information request is stored on a Cloud based Server. By redirecting this information to a new specified location, it is possible to use the Cayla Doll as a "spy device" capable of using the internal microphone to record.

Vivid Toy Group who manufacture the Doll have previously said examples of hacking were isolated incidents that were carried out by specialists and were looking into upgrading the Cayla Doll App. As a result, several upgrades of the App are now available for download.

However, due to vulnerabilities that are detailed in this poster, and as well as other known Bluetooth vulnerabilities [4], that are now associated with the Cayla Doll, it has been classified as "illegal espionage apparatus" by Germany's Federal Network Agency. This is because under German law it is illegal to manufacture, sell or possess surveillance devices disguised as another object. As a result, parents have been ordered to destroy or disable the smart doll's internal microphone, because the toy can be used to illegally spy on children.

To date, the manufacturer of the Doll: Vivid Toy Group have not responded to requests for a comment on the German ruling.

References

[1] "My friend Cayla," 2014. [Online]. Available: http://myfriendcayla.co.uk/Cayla. [Accessed 30th April 2017]

[2] "DBeaver 4.0.6," 2017. [Online]. Available: http://dbeaver.jkiss.org/download/ [Accessed 30th April 2017]

[3] "APKTool 2.2.2," 2017. [Online]. Available: https://ibotpeaches.github.io/Apktool/. [Accessed 30th April 2017].

[4] "The Guardian," 17th February 2017. [Online]. Available: https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children . [Accessed 30th April 2017].