Recommendations to Enhance Usability and Privacy of Smart Toys

Benjamin Yankson
University at Albany,
State University of New York
Albany, NY, United States
byankson@albany.edu

André de Lima Salgado
ICMC, University of São Paulo
São Carlos, SP, Brazil
alsalgado@usp.br

Renata Pontin M. Fortes
ICMC, University of São Paulo
São Carlos, SP, Brazil
renata@icmc.usp.br

Abstract

The collection of personal information by smart toys causes various privacy concerns. The use of personal information has also been subject to regulatory acts by different governments. For these reasons, smart toy manufacturers need to develop effective privacy controls. However, designing usable privacy controls remains a challenge. In this paper, we sought to identify the main security vulnerabilities involved with smart toys that are related to usability and may impact users' privacy. To this end, we performed a security analysis and usability heuristic evaluations. After identifying current vulnerabilities, we create a list of design recommendations aiming at enhancing both the usability and privacy of smart toy privacy controls. We also suggest a revised severity scale to help to prioritize the design solutions.

1. Introduction

The Internet of Things (IoT) is an ecosystem that is transforming all devices to build a smart society [1]. These smart devices have benefited consumers in many ways, such as smart thermostats placed in the home and wearable technology to monitor health and fitness [2]. IoT has also influenced children's toys that have transformed from simple, stuff toys to Internet-connected toys that can also communicate and interact with children [3], [4]. For example, Hello Barbie, an Internet-connected toy from ToyTalk.com and Mattel, operates when the button in the belt buckle is pressed, and it connects the Hello Barbie doll to the Cloud server of ToyTalk.com [5]. CogniToys Dino is another smart toy powered by IBM Watson technology that is Cloud-connected and operates through the Internet. Dino works simply as when the child asks questions by voice, and Dino that is connected to the Internet listens and replies according to the question [6]. These devices can provide personalized based services to users by collecting data from user contexts such as location, time, and weather. The Elemental Path has described the functionality of CogniToys Dino as that it gathers child personal behavior and preferences such as favorite color, favorite games and provides service according to their age-appropriate content to interact with them [7]. However, the collection and use of such sensitive information are subject to regulatory acts, such as the Children's Online Privacy Protection Act (COPPA), from the United States Federal Trade Commission [8], and the General Data Protection Regulation (GDPR), from the European Union [9]. Also, users (or their legal guardians) may not consent to such devices collecting their personal information. Therefore, smart toy manufacturers are required to implement effective privacy controls to protect the collected information [4, 10, 11].

We have seen in recent years, several privacy violations or data breaches, such as the VTech breach that resulted in the disclosure of about 6 million children records [12]. Table 1 presents some well-known children's privacy violations due to ineffective security control or privacy malpractice and their respective related fines, in US dollars, levied by United States Federal Trade Commission (FTC) against the company violating children's privacy.

Company	Violation	Year	Fine
ByteDance	COPPA compliance failure with their TikTok app.	2019	$5.7 million
Oath	COPPA violation - Online advertising.	2018	$5.0 million
inMobi	COPPA violation - location tracking.	2016	$950,000

Table 1. Some Known Privacy Violation and Fines.

Although the FTC continues to levy hefty fines against companies violating COPPA, adopting effective privacy controls remains a challenge in the field [13]. To address this challenge, we sought to review the main security vulnerabilities of some current smart toys and their

URI: https://hdl.handle.net/10125/70840
978-0-9981331-4-0
(CC BY-NC-ND 4.0)

resulting user privacy concerns and impact. For this reason, we identified security and usability problems that remain present in popular smart toy applications, causing vulnerabilities. To overcome these problems, we present a list of recommendations for further improvements in smart toy technologies.

This paper is organized as follows: Section 2 presents the background on smart toys, information security, privacy, and usability. Section 3 describes the method of this study. Section 4 presents the case studies we performed to reach our goal. Section 5 presents recommendations for future designs of smart toy privacy controls. Finally, Section 6 concludes our paper and discusses future works.

2. Background

As shown by Albuquerque et al. [14], although privacy is difficult to define, it relates to the right of people to keep their personal information a secret or not. It generally refers to one's desire to set who has access to them. This is closely related to the concept of confidentiality, which is defined by ISO 27000 as the "property that information is not made available or disclosed to unauthorized individuals, entities, or processes." In this context, confidentiality is an extension of privacy but focuses on how the user's private information is managed to prevent unauthorized users from gaining access. Essential security controls established in ISO 27001 required to maintain confidentiality can be considered as very important in establishing and protecting privacy.

The literature has diverse approaches focusing on the privacy and security issues of IoT devices, among which smart toys have an increasing interest. Hung et al. identified privacy requirements at the legislative level and privacy laws that are applicable to children's smart toys. They showed that, as the physical safety of a child is mandatory, a framework was needed to attain the privacy of the child by reducing the sensitive data collection and its retention. This included a parent or guardian to control their child-sensitive data [15]. Meanwhile, Rafferty et al. proposed a conceptual model of privacy rule for smart toys, IoT devices, and mobile services. In the model, parents and legal guardians are owners of child information, which is in accordance with a data privacy act known as COPPA (Children's Online Privacy Protection Act). COPPA allows parents and legal guardians to monitor and regulate the information that is gathered online. Parents must give their consent to rules (access rules) about sharing their child's personal data [10].

McReynolds et al. conducted a survey on parents and children who play with internet-enabled toys. They emphasize the survey on worries that parents and their children have when playing with smart toys, observing that many children were not even aware that their conversations are being recorded. They have pointed out that the toy designers should design toys in a way that alerts children before recording instead of the red blinking light that is not spotted by children. They have also suggested to toy manufacturers not to keep the recordings of child conversations for a long time and delete them in a week or allow parents to delete the recorded conversations permanently. Their study also found that many parents require parental control over the toy, such as the function to turn off the Internet on the toy or to manage its responses to children's questions [4]. Dhanhani et al. suggested that toy manufacturers should consider forensic measures while designing internet-enabled toys [16]. Rafferty presented an access control model and framework intended to protect the location of children playing with Internet-connected toys [17].

Finally, Holloway et al. [18] show the potential benefits of smart toys (e.g., enthusiasm and enjoyment). Meanwhile, they outline various emerging privacy and security issues found in smart toys. According to them, ToyTalk (responsible for the Hello Barbie) argues that it is not possible to prevent children from providing personal information. Nevertheless, ToyTalk's policies state that if the company comes across any recordings with personal information, the company will delete it. In this sense, Holloway et al. argue that the security protection of smart toys depends on parental choice over parental control. Also, they argue that this may involve other security breaches.

2.1. Privacy and Smart Toys

As per Hung et al. [3], a smart toy is:

> a device consisting of a physical toy component that connects to one or more toy computing services to facilitate gameplay in the Cloud through networking and sensory technologies to enhance the functionality of a traditional toy.

Smart toys establish two-way communication with the child [10]. The smart toy vendor is able to provide personalized based services through the collection of data from users' contexts. Smart toys often gather the childs' personal behavior and preferences, such as favorite color, favorite game, and in order to provide age-appropriate content for the child to interact with the toy. By interacting with smart toys, the toy can gather personalized information about the child. In most cases, the guardian and the child both have no idea of the concept of privacy and how to protect it. Consequently, children reveal their personal information while playing with these toys without the awareness of the dangers of such information revel [10]. The personal information

used and collected by these connected devices can be hacked; as such, sparking various security and privacy concerns. The concerns become exponential with respect to sensitive personal information about children, as all interactions of a child with the Internet-enabled toy are stored somewhere else on a remote server [10]. Because of the challenging nature of privacy and connected devices, some manufacturers of smart toys may not design security and privacy as a top requirement.

The literature shows that some smart toys available on the market remain with security threats. Mattel Hello Barbie, My friend Cayla and i-Que robot are examples of such toys [19]. For instance, parental control is needed for the proper functioning and more security of the toy [10, 16]. Hello Barbie is designed to be the child's best friend, talking and sharing secrets [18, 20]. The doll has built-in features that record every conversation between child and Barbie and stores this conversation in a cloud database. This database is also shared with the child's parents, which gives the impression that parents (or legal guardians) have absolute control over the conversations. Hello, Barbie application also includes a feature to share the recordings of children's conversations with the toy on social networks. As a matter of fact, there is a possible threat to sharing the collected data with third parties. This indicates that in both ways, Hello Barbie is not keeping a secret [18, 20].

Holloway and Green [18] discuss that security specialists can easily get access to the names of all Wi-Fi networks to which the toy connects, the user account details, and even the sound files of pre-recorded responses of Barbie conversations when the doll is not connected to the Cloud. In 2015, VTech Electronics LLC, a company that develops connected tablets for children, suffered a data breach of almost 6 million children and 4 million parents all over the world [12]. The information included parents' and child names, birthdate, pictures, gender, and account password. VTech failed to protect the Personally Identifiable Information (PII) of parents and their children that they have collected for the use of their connected tablets [21, 32]. However, these kinds of data breaches elevate concerns about the privacy of users' data; and rightful question whether these smart toy manufacturers are considerably doing enough to implement security controls necessary to address privacy risks of the collected consumer data.

According to the privacy policy of CogniToys Dino [22], the Personal Information provided by parents about themselves and their children may include name, home address, contact information, current location, email address. As one can see, this information is privacy sensitive and sufficient to identify users. The policies state that information is only used for the internal purpose, to give a personalized experience to users, and that the toy company is not going to reveal customers' collected Personal Information to third parties without the consent of users, except as described in their Privacy Policy. This may allow the company to disclose some information to third parties without identifying the identity of the parent or child. For example, to attest that smart toy companies are considering the privacy of children's information in their care, a Ranking Member, Nelson, of the US Senate, requested the security and privacy policies from few famous connected devices and toy companies. He also requested information about how they collect, use, and secure user personal information. The companies in question provided him with the report that reveals the smart toys gather much information, including the Personal Identifiable Information of parents and their children. The companies also showed that they have security policies for user data protection applied. However, the security vulnerabilities in Fisher-Price Smart Toy Bear uncovered that they were unsuccessful in protecting and securing customer data. These incidents elevated questions of whether smart toy manufacturing companies are considering the security of consumer data as their top priority [21].

Due to privacy concerns related to smart toys, studies have analyzed the security of these devices in order to identify vulnerabilities. Somerset Recon Inc [23] analyzed the security of Hello Barbie, one of the first smart toys to become popular in the market. They have identified security vulnerabilities that can be considered as privacy vulnerabilities due to its impact on privacy, as we present in Table 2. A similar security analysis is made available by Pen Test Partners [24] on the Dino smart toy, another popular smart toy in the market. We also included these analyses in Table 2.

#	**Information Security Vulnerabilities**	**Privacy Impact**
1	"*Weak passwords*" [23].	This vulnerability will allow attackers to brute force user account credentials remotely and infiltrate victim user accounts. However, we have found that this issue has been resolved now.
2	"*No Password Brute Force Protections*" [23].	This vulnerability allows attackers to brute force user mobile app account passwords remotely and infiltrate victim user accounts. An attacker is also able to gain access to audio conversations of the

		toy with a child as it is accessible through user accounts. However, as we observed, it has been resolved now.
3	"*Hello Barbie device uses unencrypted Wi-Fi network*" [23].	This vulnerability allows attackers to perform a man in the middle attack by joining open and unencrypted Barbie's Wi-Fi network. However, this Wi-Fi connection is only available in pairing mode by pressing two buttons on the device. There is a possibility that the child might unknowingly press these two buttons and open the Wi-Fi device network. We observed that this vulnerability had not been resolved by now.
	"*Hello Barbie device does not require unique authentication to modify the configuration of the device*" [23].	This vulnerability could cause the toy to use an account created by the attacker, and in this way, an attacker can listen to audio conversations. An attacker could also gain access to the user account credentials from the toy web application and insert malicious audio conversation files to the victim user account [23]. However, we observed that it had been resolved now.
4	"*Audio files can be accessed without authentication*" [23].	An attacker can get the URL of an audio conversation that is stored on CloudFront without authentication, and the file is accessible even if the user changes the account password. The problem faced by an attacker while accessing those audio conversation files would be that URL paths to all audio files are random [23]. We observed that this security vulnerability had not been resolved yet.
5	*Cross-Site Scripting:* The web Interface of the toy, which is available over Wi-Fi and is used in configuration mode, is vulnerable to a few security issues. This includes persistent Cross-Site Scripting (XSS) attack [24].	The web page does not perform input validation or sanitization while entering the SSID, and by submitting the script such as "*<script>alert (1) </script>*" [31], the code gets executed and displays "1". An attacker could exploit this vulnerability and perform Persistent XSS and Cross-Site Forgery Request attacks. As we observed, this security vulnerability has not been resolved yet.
6	*Use of HTTP for transferring sensitive information:* The web interface of the toy is used to add or modify Network SSID. The SSIDs that are in use or to set a new SSID with different priority levels are displayed on the web interface. The users can select any security type and enter a password to connect to SSIDs. This web page uses an unsecured connection HTTP, i.e., http://192.xxx.x.x, and it could be easily accessed by the hacker [24].	When the toy is in configuration mode, a hacker can perform malicious activities such as Man in the Middle (MITM) by sniffing the traffic between the user and the toy and stealing any sensitive information. However, it would be better to set login credentials to enter the web interface of the toy. As observed in our study, this security vulnerability has not been resolved yet.

Table 2. Smart toy Vulnerabilities and Privacy Impact

Although security issues are important to identify privacy vulnerabilities, studies have shown that usability also plays an important role in enhancing users' efficacy, efficiency, and satisfaction with different privacy controls [12, 25]. For this reason, in this paper, we conduct an empirical case study to evaluate the usability of examples of smart toys aiming to identify privacy vulnerabilities.

2.1.1. Usable security issues in smart toys

Recent studies have shown that usability may play an important role in enabling laypeople (as parents/guardians) to effective use of privacy controls [12], [21]. The usability concept is defined by the ISO/TR 9241 as [26] as

> the extent to which a system, product, or service can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use.

We describe a deeper relationship between usability and privacy controls by first considering the definition of usability. In regards to the usability definition, and considering the context of privacy controls, "*specified goals*" (part of usability definition) are control objectives "*(...) to be achieved as a result of implementing controls*" [27]. Because privacy controls are provided and configured by means of user interfaces, poor usability of such interfaces (e.g., because of poor effectiveness) may be seen as a weakness of the privacy control process and can be exploited by a threat. In other words, and considering that the "*weakness of an asset or control (3.14) that can be exploited by one or more threats (3.74)*" is an information security vulnerability,

poor usability of privacy controls may be seen as information security vulnerabilities [27, 28].

As the range of privacy threats increases, laypeople are often required to make security decisions [29, 41] by understanding privacy concepts or policies. However, privacy policies are usually long and complex [30], and usable tools for laypeople are still needed [12, 21]. To design usable tools of any kind, usability evaluations are essential [31]. These methods can be distinguished between those that depend on end-users to be performed (use-based evaluations) and those that depend on inspectors to be performed (inspection-based evaluations) [42]. Among inspections, heuristic evaluation (HE) is popular and allows practitioners to diagnose usability problems on the interface [33].

3. Methods

In this study, we sought to identify the main security vulnerabilities involved in the smart toys' context that have an impact on users' privacy. For this reason, we complemented the findings from a literature overview (shown in Section 2.1) with additional security analysis and two empirical usability inspections. The Security analysis stage is a security analysis of one smart toy technology to confirm the findings from the literature and, potentially, identify new issues. This stage can also confirm whether the set of security vulnerabilities is saturated, and no new vulnerabilities are found. The usability evaluation stage comprises the evaluation of two smart toy privacy controls. This is performed to identify human vulnerabilities involved with smart toy privacy controls that are due to usability aspects. To this end, we performed heuristic evaluations. Heuristic evaluations can identify information security vulnerabilities by means of employing usable security heuristics as criteria for the judgment [28]. Heuristic evaluation returns situations when users might face usability problems when setting their privacy controls. This may lead to privacy risks. Our goal is to identify usable privacy issues that can help the literature to understand how to improve the interface of smart toys' privacy controls.

3.1. Participants

Both the security analysis and usability evaluation were carried out by experts. The security analysis was conducted by two security experts (both Ph.D. students). Meanwhile, the usability evaluation was an expert review [34], conducted by two usability experts (a usability researcher, Ph.D., and a Ph.D. student). To conduct the usability evaluation of smart toys' privacy controls, we considered the privacy controls as available on current application markets. Due to time constraints, and because the literature has previous security analysis on smart toys, we only performed the security analysis on toy Alpha. For the usability evaluation, since the literature still lacks usability evaluation of privacy issues on smart toys, we performed it on both toy Alpha and Beta.

3.2. Material

We employed two smart toy technologies as a subject for the experiments. We used the "*Privacy not included*" website from Mozilla [35] to choose both smart toys. To keep the anonymity of the brands and their privacy, we refer to the technologies as toys Alpha and Beta. The smart toy brands mentioned previously in various sections of this work have no direct connection to toy Alpha or Beta used in this section of our work. Toy Alpha is a smart interactive toy that makes conversations with kids. It is connected to a Cloud-based Artificial Intelligence machine for question answering, which operates through Wi-Fi. The setting of Alpha is made available with the free app, which is available to be downloaded for Android or iOS-based phones. For feasibility reasons, the Android-based mobile app of the toys has been used throughout the case study. The Web interface of Beta had input validation errors such as Cross-Site Forgery Request and Persistent XSS. Moreover, it uses unencrypted communication channel HTTP instead of HTTPS to transmit sensitive information. It also allows weak login credentials while creating a user account. We employed toy Alpha for the security analysis and one usability heuristic evaluation.

Beta is an internet-connected toy designed and developed by a traditional toy company, and a computing company focused on talking toys. It is aimed to communicate with children, while all conversations between Beta and the child are stored in the Cloud and can be accessed or managed by parents on a dedicated website. Toy Beta can be easily configured with the application available to be downloaded for Android or iOS-based phones on their app store. We employed toy Beta for the second heuristic evaluation.

4. Results and Discussions

4.1. Security Analysis

The security analysis was based on both mobile and Web/desktop versions of a smart toy privacy control. To complement the analysis, we used the Wireshark [36] tool to clearly check what happens in the toy connection with the Cloud. The privacy vulnerabilities and their impacts are indicated in Table 3.

#	Information Security Vulnerability	Privacy Impact
1	Weak password	This vulnerability will allow attackers to gain access to users' accounts and all private and sensitive information about the user. This security vulnerability has not been resolved.
2	No Password Brute Force Protections	This vulnerability allows an attacker to brute force user passwords and infiltrate the victim user account and gain access to users' data. This security vulnerability has not been resolved.
3	Use of HTTP on the password reset web page (identified by using Wireshark)	If an attacker sniffs network traffic when the user reset its password, the attacker would be able to access the password reset page and hijack the user's account. As observed in our study, this security vulnerability has not been resolved yet.

Table 3.Vulnerabilities and related Privacy Impact

Our analysis could only find the three vulnerabilities, as listed in Table 3. Because all of these vulnerabilities were previously identified in the literature, we assumed that the set of vulnerabilities is saturated, and no further analysis is necessary at the moment.

4.2. Heuristic Evaluation I

For the first heuristic evaluation, we evaluated the Web browser-based application of privacy control for toy Alpha. We adopted the heuristics of Jaferian et al. [37] as usability criteria to inspect the privacy control. As indicated in Salgado et al. [38], these are the most appropriate usability heuristics for inspections of parental privacy controls of smart toys. All of the potential usable security vulnerabilities are new (diagnosed in our study) and were not resolved yet. They are described in Table 4.

#	Usability Problem (Information Security Vulnerability)	Reference
1	*No alternative audio description:* Users can only review the conversation content by listening to the audio files. Users may have to review large audio conversation files to identify a child's privacy breaches. This may be effortful for them.	Heuristic #1—Visibility of activity status [37]
2	*Excessive visibility for recommended audios:* Users may only review recommended audio conversation files because they are on the principal page of the Web application.	Heuristic #1—Visibility of activity status [37]
3	*Repetitive security tasks:* There is no clear way of identifying which audio conversation files have already been reviewed by users.	Heuristic #2—History of actions and changes on artifacts [37]
4	*Poor visibility of privacy policies after login:* Right after login, users are required to set up the child's information and connect the toy. During this task period, there is no indication of privacy policies ("*Provide rules and constraints*" [36]) if they need to review it.	Heuristic #4—Rules and constraints [37]
5	*Lacking audio control:* Users cannot control the audio execution ("*analyze historical information*" [36]). If they need to go to a specific part of the audio, they must listen to the entire audio until it.	Heuristic #2—History of actions and changes on artifacts [37]
6	*Excessive deletion:* Users unable to delete parts of the file ("*limit the awareness*" [36]) that may contain sensitive information of the audio conversation. Instead, they must delete the entire audio.	Heuristic #1—Visibility of activity status [37]
7	*Poor keyboard navigation:* Users may face difficulties to navigate using the keyboard ("*allow the incorporation of a workflow*").	Heuristic #5—Planning and dividing work between users [37]

Table 4. Alpha - Usability Problem and Reference.

As indicated in Table 4, most (three out of seven) of the usability problems relate to the *Heuristic #1—Visibility of activity status* [37], followed by *Heuristic #2—History of actions and changes on artifacts* [37] (two out of seven). To some extent, this was expected because usability heuristics are usually ordered according to its explanatory power [39]. Although we could perform the heuristic evaluation to identify the vulnerabilities, rating a severity for the findings was not an easy task. Because all of the issues are related to information security, highly important to the application, we could not rate the

severity of problems employing the traditional severity scale as presented by Nielsen [40]. For this reason, in Section 5, we recommend the use of a revised severity scale, which we created to address the characteristics of usability problems in privacy control tools.

4.3. Heuristic Evaluation II

For the usable security evaluation of Toy Beta, we adopted its free mobile app for iOS devices. As for heuristic evaluation, We adopted the heuristics of Jaferian et al. [36] as usability criteria to inspect the usability of toy Beta privacy control. All of the potential human vulnerabilities are new (diagnosed in our study) and were not resolved yet. They are described in Table 5.

#	**Usability Problem (Information Security Vulnerability)**	**Reference**
8	*Lacking help with password strength:* There is no indication of password strength while users are creating it. This is necessary to support the "*freedom to choose different paths that respect the constraints*" [37]	Heuristic #4—Rules and constraints [37]
9	*Lacking indication of password requirements:* There is no indication of password requirements (e.g., number of characters) while users are creating it.	Heuristic #1—Visibility of activity status [37]
10	*Privacy Policy on the external website:* The app opens its privacy policies on an external website without providing any advertisement in advance to users.	Heuristic #4—Rules and constraints [37]
11	*Lacking visibility for the privacy policy link:* The privacy policy link receives less visibility than account information and the next button. Because this is a sensitive app, privacy policies should receive more visibility.	Heuristic #4—Rules and constraints [37]
12	*Confusing user profile creation:* The app does not indicate that the account (being created) belongs to the parents/guardians and not to their children.	Heuristic #5—Planning and dividing work between users [37]
13	*Lacking privacy notice:* The app does not inform users when sensitive child information is being sent to the Cloud.	Heuristic #1—Visibility of activity status [37]
14	*Lacking cancelation of information sharing:* The app does not provide an option to cancel (undo) information sharing. After users insert children's names and dates of birth, there is no alternative to cancel it before the app sends it to the Cloud.	Heuristic #2—History of actions and changes on artifacts [37]
15	*Lacking information about the connection with mobile Artificial Intelligence (AI) assistant:* The app offers a connection with mobile AI assistance, but there is no clear explanation of what information the assistant can access.	Heuristic #1—Visibility of activity status [37]
16	*Menu lacking the option to manage a child's information:* The app asks for both parents' and child's information, but there is no indication of where to manage the child's information after its insertion.	Heuristic #2—History of actions and changes on artifacts [37]

Table 5. Beta- Usability Problem and Reference.

As one can see, we diagnosed two times more usability problems with the privacy control of toy Beta in comparison with toy Alpha. This fact does not mean that the privacy control of toy Beta is worse than the privacy control of toy Alpha. As we understand, this is due to the fact that toy Beta provides privacy control with more information about privacy policies. On the one hand, it is important to provide all the necessary information for users about their information privacy. On the other hand, this may implicate more problems related to *Heuristic #4—Rules and constraints* [37]. As indicated by Table 5, most of the problems found were related to the *Heuristic #4—Rules and constraints* (three out of nine problems) or to the *Heuristic #1—Visibility of activity status* (three out of nine problems). From these findings, we raise the question if privacy controls with more policy descriptions are prone to more situations that may contradict the *Heuristic #4—Rules and constraints*. Future research can investigate this topic. As in the heuristic evaluation of toy Alpha, the second most preferred heuristic in this evaluation was also *Heuristic #2—History of actions and changes on artifacts*. It seems that The first two heuristics of Jaferian et al. [37] are, indeed, those with the highest explanatory power, justifying the order of heuristics.

5. Recommendations for the Design of Usable Privacy Controls

In this work, we list nine information security vulnerabilities. Six out of these nine vulnerabilities are retrieved from the literature, while the other three were identified by us in this work. These vulnerabilities are not usability related and motivate us to recommend attention for further development of smart toy privacy controls by means of: (i) do not use HTTP for transferring sensitive information; (ii) validate and sanitize input to avoid Cross-Site Scripting (XSS); (iii) require encrypted Wi-Fi; (iv) protect against remote brute force attacks on users' passwords; and (v) require authentication prior to privacy control.

Although these recommendations are important, we are not the first to reinforce the importance of them since they are mostly based on the literature. On the contrary, all the 16 human vulnerabilities discussed in this study comes from our study. From these findings, we raised the question if privacy controls with more policy descriptions are prone to more situations that may contradict the *Heuristic #4—Rules and constraints*. Future research can investigate this topic. From these vulnerabilities, we suggest recommendations to improve the usability of smart toy privacy controls. These recommendations are a result of applying the heuristics of Jaferian et al. [37] in the heuristic evaluations of this study. We present the recommendations in Table 6, along with its sources, which are the usability problems, as numbered (#) in tables 4 and 5, that justify the recommendations.

Recommendation	**Usability Problem (#)**
Provide alternatives to efficiently perceive privacy controls. Users should not be obligated to interact with privacy controls by audio if they find the text more efficient to review information.	#1
Perception of control over the perception of information: The main focus of privacy controls should be on providing the perception of the control instead of providing the perception of the information collected. Users should not perceive excessive information competing with control options.	#2
Apply the ***Heuristic #2—History of actions and changes on artifacts [36]*** to provide users with the perception of which information is in accordance with users' control preferences.	#3
Provide privacy policies access at every screen and keep them consistent with the interface design.	#4, #10
Provide flexible controls. Users should be able to opt for fine-grained controls, such as deleting specific sections of the audio.	#5, #6
Provide efficient controls, such as supporting keyboard navigation for experienced users.	#7
Nudge users towards the creation of strong passwords.	#8, #9
Provide privacy notices about ongoing data sharing.	#11, #13
Clearly distinguish settings for children's information from parent's (or legal guardians') information. This is due to the need to provide information about the child, who is the smart toy user, and parents (or legal guardians) for authentication in the privacy control.	#12, #16
Provide clearly indicated alternatives to undo unwanted data sharing. This is to mitigate the consequences of laypeople giving wrong consents. Although this seems impossible, because we cannot affirm that the data has not been seen by anyone else, provide ways to request data deletion from a third party.	#14
Provide efficient control connection with artificial intelligence assistants. Users should know what information the assistant can access, and voice interactions should be human-like conversations.	#15

Table 6. Recommendations to Enhance Usability and Privacy of Smart Toys.

In the growing market of smart toys, security gets critical as users may be children and novices to the cyber world hidden behind the attractive toys. Because of the sensitive nature of children's personal information, a toy manufacturing company should design smart connected toys with security as a priority. Investment in robust security and continued updates to security measures are critical. Toy manufacturing companies should also apply acceptable data privacy practices such as a collection of only data that is required for the main operations of the smart toy and to retain collected information for the only limited time that is necessary with valid reasoning. Our recommendations aim to support companies in the design process for better smart toy privacy controls.

In addition to our recommendations, and based on our experience with the case studies, we understand that a new severity rating scale is necessary to fully indicate the severity of usable privacy problems. We need a severity rating scale that represents privacy implications in it, along with usability issues. For this reason, we adapted Nielsen's severity scale [40] to suggest the new usable privacy severity scale:

1. *Cosmetic*: usability problems, not related to policy generation/agreement, that may not stop users from using the interface.
2. *Minor*: usability problems, not related to policy generation/agreement, that may stop users from using the interface
3. *Major*: This leads to generating a wrong policy.
4. *Catastrophe*: leads to agreeing with the wrong policy.

Although new, our severity scale is based on Nielsen's [40] traditional severity scale. This might influence practical aspects of employing our new scale because it keeps the span of four levels and lean descriptions. Nevertheless, future studies are still necessary to validate our severity scale in empirical experiments.

6. Conclusions

In this paper, we sought to provide recommendations aiming to enhance the usability and privacy of smart toy privacy controls. To this end, we identified security and usability problems that remain as vulnerabilities in popular smart toy applications. From nine information security vulnerabilities, which include the literature (see Table 2), we recommend five security practices in Section 5. From the 16 usability problems identified in our study, we composed a list of 11 usable security design recommendations to enhance the privacy aspects of smart toys, as presented in Table 6. Our recommendations may be used along different stages of design, from initial requirements to evaluation (testing stage) criteria. In addition, we also create a new severity scale focused on usability problems in the context of privacy policies.

Future studies may diagnose additional problems from similar IoT applications and evolve our recommendations towards a standard. They can also explore the use of our recommendations as criteria for usability inspections in the domain, which may include the revised severity rating scale.

7. Acknowledgments

This study was supported by the grant 2017/15239-0 and 2018/26038-8, São Paulo Research Foundation (FAPESP). Also, this study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001.

8. References

[1] R. C. Motta, K. M. de Oliveira, and G. H. Travassos, "On challenges in engineering IoT software systems," in Proceedings of the XXXII Brazilian Symposium on Software Engineering - SBES '18, Sao Carlos, Brazil, 2018, pp. 42–51.

[2] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," Future Gener. Comput. Syst., vol. 78, pp. 544–546, Jan. 2018.

[3] P. C. K. Hung, J. K. T. Tang, and K. Kanev, "Introduction," in Computing in Smart Toys, J. K. T. Tang and P. C. K. Hung, Eds. Cham: Springer International Publishing, 2017, pp. 1–5.

[4] E. McReynolds, S. Hubbard, T. Lau, A. Saraf, M. Cakmak, and F. Roesner, "Toys That Listen: A Study of Parents, Children, and Internet-Connected Toys," in Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, New York, NY, USA, 2017, pp. 5197–5207.

[5] "Hello Barbie," Hello Barbie. [Online]. Available: http://hellobarbiefaq.mattel.com/. [Accessed: 29-Jan-2019].

[6] "Connected Smart Toys from Cognitoys | Order Yours Today!," CogniToys. [Online]. Available: https://cognitoys.com/. [Accessed: 29-Jan-2019].

[7] L. Ulanoff, "Smart Dino Toy is powered by a supercomputer," Mashable. [Online]. Available: https://mashable.com/2015/02/16/smart-dino-toy-powered-by-ibm-watson/. [Accessed: 29-Jan-2019].

[8] "FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information By Amending Children's Online Privacy Protection Rule," Federal Trade Commission, 19-Dec-2012. [Online]. Available: https://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over. [Accessed: 25-Sep-2017].

[9] "Art. 8 GDPR – Conditions applicable to child's consent in relation to information society services," General Data Protection Regulation (GDPR).

[10] L. Rafferty et al., "Towards a Privacy Rule Conceptual Model for Smart Toys," in Proceedings of the 50th Hawaii International Conference on System Sciences, 2017.

[11] A. K. Ghosh, K. Badillo-Urquiola, S. Guha, J. J. LaViola Jr, and P. J. Wisniewski, "Safety vs. Surveillance: What Children Have to Say About Mobile Apps for Parental Control," in Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, New York, NY, USA, 2018, pp. 124:1–124:14.

[12] B. Nelson, "Children's Connected Toys: Data Security and Privacy Concerns," Off. Overs. Investig. Minor. Staff Rep. US Senate Comm. Commer. Sci. Transp., 2016.

[13] F. Paci, A. Squicciarini, and N. Zannone, "Survey on Access Control for Community-Centered Collaborative Systems," ACM Comput Surv, vol. 51, no. 1, pp. 6:1–6:38, Jan. 2018.

[14] O. P. Albuquerque, M. Fantinato, J. Kelner, and A. P. Albuquerque, "Privacy in smart toys: Risks and proposed solutions.", Electronic Commerce Research and Applications, vol. 39, 100922, 2020. https://doi.org/10.1016/j.elerap.2019.100922 , url: https://www.sciencedirect.com/science/article/pii/S1567422319300997?casa_token=iNn9PsnJu88AAAAA:ijq22yvUHeSLB_xCLM7j848VdprRrD9U7lUAI6HQ8agq9mXEuQQsP0hjvW12bWK-WkkaDvpkSQ#f0025

[15] P. C. Hung, M. Fantinato, and L. Rafferty, "A Study of Privacy Requirements for Smart toys. " in PACIS, 2016, p. 71.

[16] M. A. Dhanhani, B. AlRasebi, A. A. Nuaimi, M. S. Students, and D. F. Iqbal, "Forensics of" Hello Barbie" Smart Toy," p. 8.

[17] L. Rafferty, "A location privacy model and framework for mobile toy computing," Thesis, 2015.

[18] D. Holloway and L. Green, "The Internet of toys," Commun. Res. Pract., vol. 2, no. 4, pp. 506–519, Oct. 2016.
[19] S. A. Millar, T. P. Marshall, N. A. Cardon, H. Llp, and G. Street, "The Toy Association White Paper on Privacy & Data Security: New Possibilities and Perils," p. 30.
[20] "ToyTalk | Legal | Terms of Use." [Online]. Available: https://www.toytalk.com/hellobarbie/terms/. [Accessed: 22-Jan-2018].
[21] M. A. Sasse, M. Smith, C. Herley, H. Lipford, and K. Vaniea, "Debunking Security-Usability Tradeoff Myths," IEEE Secur. Priv., vol. 14, no. 5, pp. 33–39, Sep. 2016
[22] "Privacy | Connected Smart Toys from Cognitoys," Cognitoys. [Online]. Available: https://cognitoys.com/pages/privacy. [Accessed: 22-Jan-2018].
[23] S. R. Inc., "Hello Barbie Initial Security Analysis," 2016.
[24] "Jurassic Poke: Hacking a Dino toy | Pen Test Partners." [Online]. Available: https://www.pentestpartners.com/security-blog/jurassic-poke-hacking-a-dino-toy/. [Accessed: 29-Jan-2019].
[25] E. Bertino, "Data Security and Privacy: Concepts, Approaches, and Research Directions," in 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), 2016, vol. 1, pp. 400–407.
[26] "ISO 9241-11:2018(en), Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts." [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en. [Accessed: 10-Dec-2018].
[27] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), "ISO/IEC 27000:2018(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary", 2018.
[28] A. Jøsang, B. AlFayyadh, T. Grandison, M. AlZomai, and J. McNamara, "Security Usability Principles for Vulnerability Analysis and Risk Assessment," 2007, pp. 269–278.
[29] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," J. Comput. Syst. Sci., vol. 80, no. 5, pp. 973–993, Aug. 2014.
[30] L. A. De and E. von Zezschwitz, "Usable privacy and security," It - Inf. Technol., vol. 58, no. 5, pp. 215–216, 2016.
[31] K. Hornbæk, "Dogmas in the assessment of usability evaluation methods," Behav. Inf. Technol., vol. 29, no. 1, pp. 97–111, 2010.
[32] B. Yankson, F. Iqbal, S. Aleem, B. Shah, P. C. K. Hung and A. P. de Albuquerque, "A Privacy-Preserving Context Ontology (PPCO) for Smart Connected Toys," 2019 12th CMI Conference on Cybersecurity and Privacy (CMI), Copenhagen, Denmark, 2019, pp. 1-6.
[33] J. Lazar, Research methods in human-computer interaction, 2nd edition. Cambridge, MA: Elsevier, 2017.
[34] A. S. for P. Affairs, "Heuristic Evaluations and Expert Reviews," 09-Oct-2013. [Online]. Available: how-to-and-tools/methods/heuristic-evaluation.html. [Accessed: 08-May-2019].
[35] Mozilla, "*Privacy Not Included: A Buyer's Guide for Connected Products," 2018. [Online]. Available: https://foundation.mozilla.org/en/privacynotincluded/categories/Toys & Games/. [Accessed: 05-Dec-2018].
[36] "Wireshark Developer's Guide." [Online]. Available: https://www.wireshark.org/docs/wsdg_html_chunked/index.html. [Accessed: 29-Jan-2019].
[37] P. Jaferian et al., "Heuristics for Evaluating IT Security Management Tools," Human-Computer Interaction, vol. 29, no. 4, pp. 311-350, 2014.
[38] A. L. Salgado, R. P. M. Fortes, R. R. Oliveira, A. P. Freire, "Usability heuristics on parental privacy controls for smart toys: From an exploratory map to a confirmatory research," Electronic Commerce Research and Applications, vol. 42, 100984, 2020, https://doi.org/10.1016/j.elerap.2020.100984. url: http://www.sciencedirect.com/science/article/pii/S1567422320300612
[39] J. Nielsen, "Enhancing the explanatory power of usability heuristics.", Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1994.
[40] J. Nielsen, "Severity Ratings for Usability Problems," 1995. [Online]. Available: https://www.nngroup.com/articles/how-to-rate-the-severity-of-usability-problems/. [Accessed: 08-Oct-2017].
[41] B. Yankson, F. Iqbal, and P. C. K. Hung, "Privacy Preservation Framework for Smart Connected Toys," Computing in Smart Toys, pp. 13-164. 2017
[42] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), "ISO/IEC 25066:2016(en), Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Common Industry Format (CIF) for Usability — Evaluation Report," 2016.