Security Tests for Smart Toys

Luciano Gonçalves de Carvalho[1,2] and Marcelo Medeiros Eler[1]
[1]*School of Arts, Sciences and Humanities, University of São Paulo, Brazil*
[2]*FATEC Mogi das Cruzes, São Paulo State Technological College, Brazil*

Keywords: Smart Toys, Toy Computing, Security, Security Tests, Security Analysis.

Abstract: Smart toys are becoming more and more common in many homes. As smart toys can gather data on the context of the user's activities (e.g., voice, walking, photo, etc.) through camera, microphone, GPS and various sensors and store personalized and confidential information (e.g., location, biography information, activities pattern, etc.), security measures are required to assure their reliability, specially because they are mainly used by vulnerable users, children. In fact, several security flaws have been reported on smart toys available in the market. Security incidents include information leakage, toys used as spies and outsiders interacting with children via unauthorized connections. Some researchers have investigated smart toys vulnerabilities and risks when it comes to security issues, many of them have studied how to assure privacy policies compliance, and one researcher proposed general security requirements for smart toys. However, no work has proposed general security analysis and tests to assure security requirements have been met. In this context, this paper discusses security issues, threats and requirements in the context of smart toys and presents general security analysis and tests for smart toys, all identified based on the Microsoft Security Development Lifecycle (SDL) process. We believe this work contributes to this field by providing manufacturers, developers and researchers with a general guideline on how to handle security aspects when designing and developing smart toys.

1 INTRODUCTION

Recently, the toy market has been provided with a new type of product: smart toys. A smart toy is a combination of three components: a conventional *physical toy*, such a stuffed pet or a robot, for instance, equipped with sensors and electronic components to enable network communication and collect data; a *mobile device* that connects with the physical toy to provide mobile services; and a *mobile application* to interact with the physical toy. Such a combination of components are intended to provide users with more pleasant and personalized experiences.

This special association between the physical toy and a mobile device has been called *toy computing* (Rafferty and Hung, 2015). To avoid any misunderstanding, in this paper we consider smart toys those that fall in the field of toy computing, which has an association between a physical toy and a mobile device and application. We don't refer to toys that are intended to help children to become smarter (e.g. puzzles) or toys with electronic parts that reacts to environment stimuli and even learn patterns based on user data and interaction (electronic toys).

Smart toys are examples of real-world objects that can be part of an Internet of Things (IoT) network, which is a pervasive and ubiquitous network that allow the interconnectivity of real-world objects. IoT networks create a suitable environment to allow the integration of physical objects into computer-based systems aiming at improving efficiency, accuracy and reduced human intervention in several domains. As computer-based systems can control and retrieve information from physical objects, information security has become one of the key concerns in IoT networks, specially when confidential data is involved.

As such, the security of smart toys has been a raising concern for users and parents, specially because they are mostly used by children (Carr, 2017), which are considered vulnerable in most countries and cultures. In fact, many countries and communities have created their own set of rules or regulations that address data protection when it comes to children interacting with online services, such as the COPPA (Children's Online Privacy Protection Act) from the USA, the PIPEDA (Personal Information Protection and Electronic Documentation Act) from CANADA, and the GDPR (General Data Protection Regulation)

Gonçalves de Carvalho, L. and Medeiros Eler, M.
Security Tests for Smart Toys.
DOI: 10.5220/0006776101110120
In *Proceedings of the 20th International Conference on Enterprise Information Systems (ICEIS 2018)*, pages 111-120
ISBN: 978-989-758-298-1

from the European Parliament and the Council of the European Union. Unfortunately, few policies have been disclosed regarding security policies for smart toys so far.

Given that the IoT market represents a huge revenue for several companies, security solutions have been proposed such as the Industrial Security Appliances (ISA) and Cisco ASA from CISCO Systems, for example. However, they are very expensive solutions and aim at more complex infrastructures. Policies and requirements have been also proposed to assure the security of mobile services and applications (Biswas, 2012; Zapata et al., 2014; Nagappan and Shihab, 2016). Nonetheless, defining such policies and requirements for smart toys requires a separate investigation since they usually run in a less secure environment, e.g. with few security controls.

A smart toy is a more vulnerable device than a mobile application because smart toys have an actual physical toy (a simpler device than a smartphone or a tablet, controlled by the mobile application) that may also collect, manipulate and store information. Moreover, it has network features to communicate with the mobile device and other computational systems, which increases the attack surface. As most smart toys are manufactured by well known and established companies, parents tend to believe their children are safe around these products. However, according to the Federal Bureau of Investigation (FBI) of the USA, parents should be worried since "security safeguards for these toys can be overlooked in the rush to market them and to make them easy to use" (FBI, 2017).

In fact, there have been several public reports on security flaws presented by best seller smart toys (Baraniuk., 2016; Hackett, 2016; Newman, 2015; Cuthbertson, 2017; Franceschi-Bicchierai, 2016; Poulter, 2017; Jones and Meurer, 2016). Security issues include, for example, information leakages (biography information, photos), toys used as spies, and outsiders interacting with children via a smart toy. Such flaws may be a threat even to the children safety since they can provide confidential information (e.g. location), and children can even unrestrictedly follow instructions given by the toy.

Such security issues motivated the FBI in the USA to raise an alert for families on the risks such toys can bring (FBI, 2017). According to them, many toys sporting cloud-backed features such as speech recognition or online content hosting "could put the privacy and safety of children at risk due to the large amount of personal information that may be unwittingly disclosed.".

In this context, it is crucial that specific measures are taken towards assuring that smart toys are safe for their users. Consequently, researchers have been working in this specific subject (Ng et al., 2015; Rafferty and Hung, 2015; Hung et al., 2016; Rafferty et al., 2017a; Yankson et al., 2017). However, they have only addressed security issues restricted to privacy and confidentiality problems that, while very important, are not the only ones. Parental control mechanisms can mitigate relevant privacy issues, however they cannot avoid attacks that compromise other security properties.

In special, regarding general proposals for security issues, we have previously identified 12 issues, 15 threats and 20 security requirements for a typical toy computing scenario (de Carvalho and Eler, 2017). This work was based on the Requirements and Design phases of the Microsoft Security Development Lifecycle (SDL) process, the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege) approach, and the COPPA and PIPPEDA regulation. However, we have not discussed how the remaining phases of SDL process – Implementation, Verification and Release – can be useful to verify and test smart toys to assure the security requirements have been met.

Therefore, this paper contributes to this particular field as follows:

- it extends our previous work by revising the issues, threats and security requirements identified for smart toys (de Carvalho and Eler, 2017), but considering the GDPR from the European Union;
- it shows how the Implementation, Verification and Release phases of the SDL process can help defining security analysis and tests for smart toys to assure the security requirements have been met;
- it presents how smart toys available in the market could have benefited from the security issues, threats, requirements, analysis and tests presented and discussed in this work.

We believe our work can contribute not only with well known smart toys manufacturers, which, in theory, have resources to invest in a specialized team to assure their products are reliable, but also with researchers and developers that wants to create reliable smart toys to be used for several purposes. For instance, researchers have designed a smart toy called EDUCERE, stackable cubes with a data collector module, as a resource to automatically detect delays in psychomotor development in children (Gutiérrez García et al., 2017). Another example is StoryTech, a smart storytelling toy that encourages children to produce their own stories by contributing to narrative activities to make a positive impact on their creativity (Kara et al., 2013).

This paper is organized as follows. Section 2 shows the background. Section 3 discusses related work. Section 4 presents issues, threats and requirements for a typical toy computing environment, while Section 5 shows the proposed security analysis and tests for smart toys. Section 6 shows how some smart toys currently available in the market could have been benefited from our work. Finally, concluding remarks and future directions are presented in Section 7.

2 BACKGROUND

This section introduces basic concepts behind smart toys and the security process used in this work.

2.1 Smart Toys

Recently, the growing interest for technological gadgets from people of all ages has promoted the development of high tech toys, also known as smart toys. A smart toy is a device consisting of a physical toy component that connects to one or more toy computing services to facilitate game-play in the Cloud through networking and sensory technologies to enhance the functionality of a traditional toy (Rafferty and Hung, 2015).

A smart toy can also use camera, microphone and various other sensors to capture voice, record videos and photos, track location and to store personalized information (Rafferty and Hung, 2015). A smart toy can be considered an Internet of Thing object which can collect contextual data on the context of the user (e.g., time of day, location, weather, etc.) and provide personalized services to enhance user's experience.

Smart toys are in general composed of three parts: a conventional physical toy (such as a car or a doll) equipped with electronic components, sensors, and software which enable wireless communication with other computational systems via Wi-Fi, Bluetooth, Near Field Communication (NFC); a mobile device that provides the smart toys with mobile services to enhance their functionalities; and a mobile application that interacts with the physical toy. Figure 1 shows an illustration of this environment including the user. Rafferty and Hung (2015) refer to this field of study as toy computing, which associates the physical computation (embed systems and sensors in a traditional toy) with mobile services.

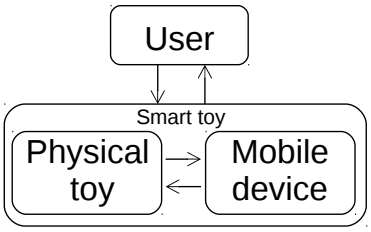

Figure 1: Toy computing environment.

2.2 The Microsoft SDL Process

Microsoft SDL (Lipner, 2004; Microsoft, 2010) stands for security software development, and aims at assuring the security of systems during the whole development process. It has the following main phases:

1. Requirements: security requirements establishment, quality gates and bug bars definition and documentation (set security and privacy minimum levels), and security and privacy risk analysis;
2. Design: design requirements establishment, attack surface analysis and threat modeling;
3. Implementation: approved tools utilization, insecure functions disable and static analysis execution;
4. Verification: dynamic analysis and fuzzing tests execution, and attack surface review;
5. Release: incident response plan elaboration, final security review execution and software release. The SDL foresees its use in conjunction with both conventional and agile software development processes (Microsoft, 2011).

Requirements identification is performed in Requirements and Design phases. In the first phase, minimum security and privacy quality levels are established through quality gates and bug bars whereas, in the design phase, security and privacy design specification is built, which describe the security and privacy features that will be exposed directly to the user. The security tests are identified based on the remaining phases: Implementation, Verification and Release.

In the Implementation phase, static analysis is performed aiming at finding security flaws on the source code. In general, the source code is automatically analyzed by tools known as Static Application Security Testing (SAST). In the Verification phase, dynamic analysis and fuzz testing are performed. Dynamic analysis simulates attacks and monitors the software aiming at finding vulnerabilities such as memory corruption and user privileges failures. Fuzz testing aims at finding general flaws in the system under test. In the Release phase, penetration tests are performed to find all sort of vulnerabilities, either when no internal information is available or when they are.

3 RELATED WORK

Researchers have been working in security aspects of smart toys since they emerged. They have been paying special attention to privacy aspects. Researchers have also investigated smart toys examples aiming at identifying risks, security flaws and vulnerabilities (Rafferty et al., 2017b; Dobbins, 2015), or simply performing general analysis of smart toys mentioning how vulnerable they are given their characteristics or how parents feel around such products (Taylor and Michael, 2016; McReynolds et al., 2017).

Rafferty and her colleagues used a formal privacy threat model to investigate privacy requirements for toy computing (Rafferty and Hung, 2015). As a result, they have compiled six (6) privacy rights (privacy requirements). In a related project, they have also proposed a privacy rule conceptual model where parents/legal guardians are the owners of their child's data and provide consent to share the data collected through access rules (Rafferty et al., 2017a).

Some researchers have discussed the seriousness of privacy implication for smart toys and surveyed related work on privacy issues within this domain (Yankson et al., 2017). They also discuss global perspectives regarding legislation on such devices and propose common best practices for parents and manufactures to assure child safety. In the same topic, Hung and his colleagues discuss related privacy requirements for smart toys in a toy computing environment with a case study on a commercial smart toy called Hello Barbie from Mattel (Hung et al., 2016).

Although many work has been done in this area, most of them focus on privacy and not in general security aspects. Moreover, most of them reports concerns about smart toys vulnerabilities but do not present any security requirements and how to ensure they have been implemented. In that sense, we previously presented a list of security issues, threats and requirements on a typical architecture of smart toys (de Carvalho and Eler, 2017). However, we do not discuss in this work how security analysis and tests should be carried out in order to check whether the security requirements have been met. Therefore, there is still room for contributions in this area.

4 SECURITY ISSUES, THREATS AND REQUIREMENTS FOR SMART TOYS

We have previously identified 12 issues, 15 threats and 20 security requirements based on the Requirements and Design phases of the Microsoft SDL process, the STRIDE approach and regulations such as PIPEDA and COPPA (de Carvalho and Eler, 2017). We have revisited and extended our previous work by considering an additional regulation: the GDPR, from the European Union. Such regulation provided us with more knowledge into how to strengthen and unify data protection for all individuals, but, in the case of our investigation, children's data. As a result, we have identified four more issues (I13 to I16) and two more security requirements (SR21 and SR22).

The whole set of security issues that should be addressed regarding smart toys according to the aforementioned regulations and standards are presented as follows:

- I1 Provide notice about information collection, use and disclosure practices.
- I2 Obtain parental consent for personal information collecting, using and disclosing.
- I3 Not promote unnecessary personal information disclosure.
- I4 Protect personal information confidentiality, integrity and availability.
- I5 Provide the same protection level for third party information processing.
- I6 Implement procedures to protect personal information.
- I7 Document the purposes for which personal information is collected.
- I8 Obtain individual consent for the personal information collection, use or disclosure.
- I9 Specify the type of personal information collected.
- I10 Retain personal information only as long as necessary.
- I11 Maintain personal information accurate, complete and up-to-date as is necessary.
- I12 Protect personal information against loss or theft, unauthorized access, disclosure, copying, use, or modification.
- I13 The request for consent must be given in an intelligible and easily accessible form.
- I14 Breach notification is mandatory and data processor are required to notify their customers.

I15 Data erasure of personal data, cease the further dissemination of the data and halt processing of the data for third parties.

I16 Inclusion of data protection from the onset of the designing of systems.

The whole set of threats concerning smart toys are presented as follows:

T1 Spoofing:

- T1.1 The children is not playing, but the attacker (insider), who wants to discover confidential information.
- T1.2 An attacker is using another mobile device to control the toy (Bluetooth parallelization).
- T1.3 The mobile service provider is fake.

T2 Tampering:

- T2.1 Unauthorized modification of the configuration file of the mobile device (loads a configuration file not suitable for the user).
- T2.2 Unauthorized modification of the information exchanged through network communication between the components (physical toy x mobile device x access point/router).
- T2.3 Unauthorized modification of the database in the mobile device (changes the game points, user's actions history, etc).

T3 Repudiation:

- T3.1 User denies purchases of services, accessories etc.

T4 Information disclosure:

- T4.1 Disclosure of personal information stored in the database.
- T4.2 Disclosure of information used to request mobile services (localization, context data etc).
- T4.3 Disclosure of information stored in the mobile device (photos, video, text messages etc).

T5 Denial of Service:

- T5.1 A service inserts enough information in the database to reach the full capacity of the mobile device storage system.
- T5.2 More than one device sends commands to the physical toy making it not able to provide the correct answer.
- T5.3 An attacker denies access to mobile services through the access point.

T6 Elevation of privilege:

- T6.1 An attacker watches the data exchanged by the network communication between the mobile device and the toy, then changes it to access the toy.
- T6.2 An attacker watches the data exchanged by the network communication between the mobile device and the mobile services, then changes it to access the mobile services.

The whole set of security requirements identified for a typical smart toy environment are the following:

SR01 The smart toy app must provide notice of what information it collects and the further use and disclosure practices.

SR02 The smart toy app must provide an specific interface in order to identify user age and obtain user consent before the personal information collection and manipulation; in the case of child user, obtain verifiable parental consent and parental consent review.

SR03 The smart toy app must not ask for more personal information in order to continue its operation.

SR04 The smart toy app must authenticate users.

SR05 Communication between physical toy and mobile device must use a protocol that allow authentication and authorization mechanisms.

SR06 Mobile services providers must own digital certificates allowing identity verification.

SR07 Configuration file integrity must be maintained and verified in every mobile app play session.

SR08 Every communication in toy computing environment must use cryptographic mechanisms.

SR09 The Database Management Systems (DBMS) must provide user authentication.

SR10 The DBMS must provide security mechanisms against to external modification of stored data.

SR11 The smart toy app must request authentication renew before every financial transaction.

SR12 The DBMS must provide data encryption feature or allow data encryption by third-party tools.

SR13 The smart toy app must encrypt personal information accessed from others apps inside the same mobile device.

SR14 The mobile app must not access unnecessary files from others mobile apps inside the same mobile device.

SR15 The mobile app must monitor and limit database growth.

SR16 The physical toy must not accept commands from mobile devices outside the current play session.

SR17 Every communication must use secure protocol with cryptographic mechanisms.

SR18 The smart toy app must show the privacy police when required.

SR19 The smart toy must delete every personal information collected that is no longer useful.

SR20 The smart toy must maintain personal information accurate, complete and up-to-date as is necessary.

SR21 The smart toy app must notify users about security breach and enable updates.

SR22 The smart toy development and updates must consider well-known security principles.

5 SECURITY TESTS FOR SMART TOYS

Following the SDL process, we have identified tests and analysis required to meet security issues and requirements identified in the previous section based on the Implementation, Verification and Release phases. As a consequence, we expect such measures to mitigate the threats we identified.

5.1 Implementation

During this phase, SAST (Static Application Security Testing) tools are used to identify security flaws in the source code. Such tools can identify when best practices for security control are not implemented. For the Android O.S., for instance, the tools QARK, Androbugs and JAADAS are commonly used in this task, for they are able to identify security flaws regarding the following classes and areas (OWASP, 2017):

- Data validation.
- Authentication.
- Session management.
- Authorization.
- Cryptography.
- Error and exception handling.
- Login procedures.
- Security configurations.
- Network architecture.

Accordingly, we have identified the security requirements that can be verified by means of a static analysis tools. Table 1 shows the security requirements and the corresponding security failure class it is related to.

Table 1: Security Requirements and related security failures classes.

Sec. Req.	Security failure class
SR04	Authentication
SR05	Authentication and Authorization
SR08	Criptography
SR09	Authentication
SR13	Criptography
SR17	Criptography
SR22	All classes

5.2 Verification

In the Verification phase, more specialized tests are required to assure that the application meets the established requirements. Therefore, each security requirement which has not been verified yet is classified, when applicable, according to one of the security test classes (OWASP, 2013):

- Configuration and Deployment management.
- Identity Management.
- Authentication.
- Authorization.
- Session Management.
- Input Validation.
- Error Handling.
- Weak Cryptography.
- Business logic.
- Client Side.

Although the presented security tests classes have not been created for mobile applications, they are generic enough to be useful in this context. Therefore, Table 2 shows each security requirement associate with a corresponding test class.

Table 2: Security Requirements and corresponding security test classes.

Sec. Req.	Test class
SR06	Weak Cryptography
SR07	Business Logic
SR10	Business Logic
SR12	Weak Cryptography
SR14	Configuration and Deployment Management
SR15	Configuration and Deployment Management
SR19	Configuration and Deployment Management

Once each security test has been associated to a security test class, it is possible to define more specific and suitable security tests required to check whether the application meet the security requirements. Following we present the general security tests applicable to this phase considering each security requirements presented at Table 2.

Security Requirement: RS06
Test: Security tests in protocols with cryptography
Description:

- Check whether the certifier authority is trustworthy.
- Check whether the certificate is valid.
- Check whether the website name is the same as the certified one.

Security Requirement: SR07, SR10
Test: Integrity verifications test
Description:

- Checks whether the application does not allow users to destroy the integrity of any part of the system or its data.

Security Requirement: SR12
Test: Cryptography test
Description:

- Check whether the files stored at the database are ciphered.

Security Requirement: SR14, SR19
Test: Application platform configuration test
Description:

- Check the configuration of each element of the application architecture.

Security Requirement: SR15
Test: Application platform configuration test
Description:

- Checks the database configuration

5.3 Release

In the Release phase it is possible to verify, by means of alpha and beta tests, all security requirements that depends on a functional prototype or version of the smart toy. Alpha tests are able to check the following security requirements: SR1, SR2, SR3, SR11, SR16 and SR18, while the beta tests are able to check the following security requirements: SR20 and SR21.

In the absence of alpha and beta tests, it is recommended that penetration tests to be used, as used in the Hcon Security Testing Framework (HconSTF), Samurai Web Testing Framework (SamuraiWTF) and Samurai Project's Security Testing Framework for Utilities (SamuraiSTFU), for instance, but tailored to the toy computing environment. Showing how to tailor such tests to the toy computing environment is not at the scope of this work.

6 SECURITY ANALYSIS AND TESTS FOR SMART TOYS AVAILABLE IN THE MARKET

We present an overview of a few smart toys available in the market aiming at providing illustration of the smart toys capabilities and specially how vulnerable they can become. Most of the smart toys uses cameras, microphone and different sensors to collect, observe or infer personal information to provide customers with more personalized game experiences. The data collected by the physical part of the smart toy are sent to a mobile device and/or a server through a wireless network. The mobile application of the smart toy running in the mobile device, in turn, gets mobile services provided by Internet servers.

Data collection may be a problem when appropriate security controls are missing because private information could be exposed in a data leakage. A quick search over the Internet for security issues in smart toys will reveal security flaws such as private information leakages and outsiders interacting with children via a smart toy (Baraniuk., 2016; Hackett, 2016; Newman, 2015; Cuthbertson, 2017; Franceschi-Bicchierai, 2016; Poulter, 2017; Jones and Meurer, 2016).

We believe the 22 security requirements previously presented address many of the general security issues related to the smart toys currently available in the market. Following we present a description of some smart toys, some publicly disclosed security flaws and some suggested requirements and test cases that could have helped prevented the reported issues.

Here, we have no intention of exhaustively exploring all security requirements and possible tests for smart toys available in the market since they have many features. The purpose is to show that many of the flaws found in such toys could have been addressed if security measures have been made since the Requirements elicitation phase of the development process. Moreover, suggested tests are generic since specific tests depends on specific architectures, programming languages, libraries, APIs, which we do not have access because they are not publicly available. A summary of the tests and analysis performed in each phase and associate requirements is presented in Tables 3, 4 and 5.

6.1 CloudPets

A CloudPet is a stuffed pet with built in capabilities and associated mobile services. Parents, relatives or friends can record and send messages using an app from anywhere in the world. A parent or guardian gets the message on their CloudPet App and then approves it and delivers it wirelessly to the CloudPet. Children can also record a message which can be delivered to a contact network anywhere in the world.

Spiral Toys, the CloudPets manufacturer, left customer data of its CloudPets brand on a database that wasn't behind a firewall or password-protected. The exposed database contained data on 821,396 registered users, 371,970 friend records (profile and email) and 2,182,337 voice messages. The voice messages were not in the database, but they were stored in an Amazon S3 bucket that doesn't require authentication. Moreover, customers used weak passwords making it trivial to log into their accounts and listen to the saved messages. One of the biggest concern in this context is that someone may be able to use disclosed information to send inappropriate messages to children and to gather information on families, friends, which may put children safety in risk.

According to our analysis, in the case of this smart toy, meeting requirements SR09 (the DBMS must provide user authentication) and SR12 (the DBMS must provide data encryption feature) would have prevented the security issues in which personal were accessed by attackers due to security flaws related to database access.

Following the SDL process, in the Implementation phase, SAST tools could be used to check requirement SR09. In the Verification phase, Cryptography test is suggested to check SR12. In the Release phase, no test is applicable to the security requirements we are considering in this example.

6.2 Smart Toy Bear

This Mattel Fisher-Price interactive learning smart toy with voice and image recognition features are capable to collect data to adapt to create personalized playing. Through the mobile app and a Wi-Fi connection, the smart toy gets updates and the parents can unlock bonus activities.

Some Internet servers may fail to authenticate users and expose data and profiles. The Smart Toy® Bear vulnerability in the backend systems enabled attackers to access private information

In the case of the Smart toy bear, implementing security requirements SR04, SR05, SR06, SR07, SR08, SR12, SR16 e SR17 would have prevented security issues caused by insecure APIs, which allowed attackers to access personal information and to send commands to the physical toy.

Table 3: Security requirements addressed by SAST tools at the Implementation phase.

Smart toy	Sec. Req.	Sec. Test
CloudPets	SR09	SAST Tool
Toy bear	SR04, SR05, SR08, SR17	
Hello Barbie	SR05, SR17	
Cayla	SR04, SR05	
I-QUE	SR04, SR05	

Table 4: Security Requirements addressed by security tests during the Verification phase.

Smart toy	Sec. Req.	Sec. Test
CloudPets	SR12	Cryptography tests
Toy bear	SR06	Security tests in protocols with cryptography
	SR07	Integrity verification tests
	SR12	Cryptography tests
Hello Barbie	SR06	Security tests in protocols with cryptography
	SR07	Integrity verification tests
	SR12	Cryptography tests
Cayla	-	Not applicable
I-QUE	-	Not applicable

Considering the SDL process, SAST tools can check security requirements SR04, SR05, SR08 and SR17 during Implementation phase. In the Verification phase, security tests in protocols with cryptography can check SR06 while integrity verification tests can check SR07 and cryptography tests the SR12. In the Release phase, an alpha test in which a user sends commands to the physical toy during a

Table 5: Security Requirements addressed during the Release phase.

Smart toy	Sec. Req.	Sec. Test	Description
CloudPets	-	Not applicable	Not applicable
Toy bear	SR16	alpha	User sends commands to the physical toy during the game session from another user.
Hello Barbie	-	Not applicable	Not applicable
Cayla	SR03	alpha	User uses all resources of the toy without providing any additional personal information.
I-QUE	SR03	alpha	User uses all resources of the toy without providing any additional personal information.

game session from another user can help checking SR16.

6.3 Hello Barbie

Another Mattel smart toy, the Hello Barbie is a doll equipped with a microphone, speaker and a speech recognition feature, allowing a two-way conversation when connected to a Wi-Fi network. A mobile app is required for account set up and allow parents to listen child's conversation with the toy. To improve conversation, the toy store conversations and sent them to a server in the Internet. Hello Barbie doll app, for example, can automatically connect to unsecured Wi-Fi networks and reveal confidential information.

In this specific smart toy, satisfying security requirements SR05, SR06, SR07, SR12 e SR17 would have avoided the exploitation of several vulnerabilities of communication interception, personal information disclosure and insecure Wi-Fi connections.

During the Implementation phase of the SDL, SAST tools can check SR05, SR17. In the Verification phase, security tests in protocols with cryptography can check SR06 while integrity verification tests can check SR07 and cryptography tests the SR12. In the release phase, no test is applicable in to the security requirements we are considering in this example.

6.4 Cayla and I-QUE Intelligent Robot

They are both smart toys from Genesis Toys that are able to answer several questions and, to improve user experience, connects to the Internet through a mobile device. Genesis Toys was accused by consumer groups in the US, among other things, of collecting children's personal data (Baraniuk., 2016). It was possible to connect to the toys from any mobile device through Bluetooth. The data exchange between physical toy and mobile device can be easily intercepted.

In the case of these two smart toys, fulfilling security requirements SR03, SR04 e SR05 would have prevented, among other security issues, that attachers requested personal information from children through non-authorized connections via Bluetooth, simply by using any mobile device nearby the smart toy.

Considering the phases of the SDL, SAST tools can check SR04 and SR05 for both toys. Tests of the Verification phase are not applicable, but in the Release phase both smart toys can benefit from using alpha tests in which a user uses all resources of the toy but providing no additional information. Such test is useful to check SR03.

7 CONCLUSIONS AND FUTURE WORK

In this paper, we presented a contribution to the smart toys field in three ways. First, we revisited our previous work (de Carvalho and Eler, 2017) to include four (4) security issues and two (2) security requirements. Next, we presented general security analysis and tests for smart toys based on the Implementation, Verification and Release phases of the SDL process, and on related security issues, threats and requirements. Finally, we presented an analysis of smart toys available in the market in which we discuss some of their security flaws publicly reported and how the security and test requirements identified in this work could have prevented some of the related flaws.

The proposed security requirements, the analysis and tests are generic and can be related to most smart toys that fits in the toy computing field, in which there is an association between a physical toy and a mobile device and application. Concrete tests depends on programming languages, specific architectures, libraries and access to the smart toys, so the contribution of this work is theoretical and general.

Even though wealthy and well known manufacturers have plenty of resources to perform a careful security analysis to identify threats and implement security features, the security flaws we discussed in this paper are presented by these manufacturers. As stated by the FBI (FBI, 2017), "security safeguards for these

toys can be overlooked in the rush to market them and to make them easy to use". In fact, many of the reported flaws could have been avoided by fulfilling simple requirements and following a process to test each security requirement.

Therefore, however theoretical, we believe the security requirements presented in this work along with the security analysis and tests might be useful not only for well known manufacturers, but also for researchers and developers who aim at creating reliable smart toys for many purposes, such as the case of the EDUCERE, the smart toy designed to help detecting delays in children's psychomotor development.

As future work, we intend to build a prototype of a smart toy to concretely implement all tests proposed for this context. Moreover, we plan to identify specific security patterns and flaws that arises from toy computing architectures.

REFERENCES

Baraniuk., C. (2016). Bbc news. call for privacy probes over cayla doll and i-que toys.

Biswas, D. (2012). Privacy policies change management for smartphones. In *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*, pages 70–75.

Carr, J. (2017). The internet of toys – the impact on children of a connected environment. *Journal of Cyber Policy*, 2(2):227–231.

Cuthbertson, A. (2017). Newsweek. internet-connected teddy bear leaks 2 million voice recordings of parents and children.

de Carvalho, L. G. and Eler, M. M. (2017). Security requirements for smart toys. In *ICEIS 2017 - Proceedings of the 19th International Conference on Enterprise Information Systems*, volume 2, pages 144–154.

Dobbins, D. L. (2015). *Analysis of Security Concerns and Privacy Risks of Children's Smart Toys*. PhD thesis, Washington University St. Louis, MO, USA.

FBI (2017). Federal bureau of investigation - consumer notice: Internet-connected toys could present privacy and contact concerns for children.

Franceschi-Bicchierai, L. (2016). Motherboard. hacked toy company vtech's tos now says it's not liable for hacks.

Gutiérrez García, A. M., Martín Ruiz, L. M., Rivera, D., Vadillo, L., and Valero Duboy, A. M. (2017). A smart toy to enhance the decision-making process at children's psychomotor delay screenings: A pilot study. *J Med Internet Res*, 19(5):e171.

Hackett, R. (2016). Fortune. this fisher-price smart toy bear had data-leak vulnerability.

Hung, P. C. K., Iqbal, F., Huang, S.-C., Melaisi, M., and Pang, K. (2016). *A Glance of Child's Play Privacy in Smart Toys*, pages 217–231. Springer International Publishing, Cham.

Jones, M. L. and Meurer, K. (2016). Can (and should) hello barbie keep a secret? In *2016 IEEE International Symposium on Ethics in Engineering, Science and Technology (ETHICS)*, pages 1–6.

Kara, N., Aydin, C. C., and Cagiltay, K. (2013). Investigating the activities of children toward a smart storytelling toy. *Journal of Educational Technology & Society*, 16(1):28–43.

Lipner, S. (2004). The trustworthy computing security development lifecycle. In *Proceedings of the 20th Annual Computer Security Applications Conference*, ACSAC'04, pages 2–13, Washington, DC, USA. IEEE Computer Society.

McReynolds, E., Hubbard, S., Lau, T., Saraf, A., Cakmak, M., and Roesner, F. (2017). 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*, CHI '17, pages 5197–5207, New York, NY, USA. ACM.

Microsoft (2010). Simplified implementation of the microsoft sdl.

Nagappan, M. and Shihab, E. (2016). Future trends in software engineering research for mobile apps. In *2016 IEEE 23rd International Conference on Software Analysis, Evolution, and Reengineering (SANER)*, volume 5, pages 21–32.

Newman, J. (2015). Pc world. internet-connected hello barbie doll can be hacked.

Ng, G., Chow, M., and Salgado, A. d. L. (2015). *Toys and Mobile Applications: Current Trends and Related Privacy Issues*, pages 51–76. Springer International Publishing, Cham.

OWASP (2013). Owasp testing guide 4.0.

OWASP (2017). Open web application security project (owasp) homepage - source code analysis tools.

Poulter, S. (2017). Daily mail - science and tech. how safe is your child? best-selling smart toys have worrying security failures that let strangers talk to your little ones without your knowledge.

Rafferty, L. and Hung, P. C. K. (2015). *Introduction to Toy Computing*, pages 1–7. Springer International Publishing, Cham.

Rafferty, L., Hung, P. C. K., Fantinato, M., Peres, S. M., Iqbal, F., Kuo, S.-Y., and Huang, S.-C. (2017a). *Towards a Privacy Rule Conceptual Model for Smart Toys*, pages 85–102. Springer International Publishing, Cham.

Rafferty, L., Iqbal, F., and Hung, P. C. K. (2017b). *A Security Threat Analysis of Smart Home Network with Vulnerable Dynamic Agents*, pages 127–147. Springer International Publishing, Cham.

Taylor, E. and Michael, K. (2016). Smart toys that are the stuff of nightmares [editorial]. *IEEE Technology and Society Magazine*, 35(1):8–10.

Yankson, B., Iqbal, F., and Hung, P. C. K. (2017). *Privacy Preservation Framework for Smart Connected Toys*, pages 149–164. Springer International Publishing, Cham.

Zapata, B. C., Niñirola, A. H., Fernández-Alemán, J. L., and Toval, A. (2014). Assessing the privacy policies in mobile personal health records. In *2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 4956–4959.