Security Requirements 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 Requirements.

Abstract: Toys are an essential part of our culture, and they evolve as our technology evolves. Smart toys have been recently introduced in our market as conventional toys equipped with electronic components and sensors that enable wireless network communication with mobile devices that provide services to enhance the toy's functionalities. This environment, also called toy computing, provides users with a more sophisticated and personalised experience since it collects, processes and stores personal information to be used by mobile services and the toy itself. On the other hand, it raises concerns around information security and child safety because unauthorized access to confidential information may bring many consequences. In fact, several security flaws in toy computing have been recently reported in the news due to the absence of clear security policies in this new environment. In this context, this paper presents an analysis of the toy computing environment based on the Microsoft Security Development Lifecycle and its threat modelling tool with the aim of identifying a minimum set of security requirements a smart toy should meet. As result we identified 15 threats and 20 security requirements for toy computing.

1 INTRODUCTION

Toys have been around for a long time in our society, either for leisure or for educational purposes. As they are fundamentally used by children, they must be designed to assure the safety of their users according to their age. Toys that can be disassembled in small parts, for example, may not be safe for babies or toddlers. That is why most toys have a clear indication of the age range they are appropriate for.

Looking forward to providing users with more interactive and personalised experiences, toy manufacturers have introduced the smart toys in the market. A distinguishing characteristic of a smart toy is that it usually has three components: a conventional physical toy equipped with sensors and electronic components to enable network communication; a mobile device that provides the physical part with mobile services; and a mobile application to interact with the physical toy. This special association between the physical toy and a mobile device has been called toy computing by Rafferty and Hung (2015).

There are other types of toys in the market that are called smart toys. One of them refers to toys that are intended to help children become smarter, such as puzzles or logic games, for example. The other one refer to toys embedded with electronic parts that can react to environment stimuli, store data or even learn patterns based on user interaction. Those are the electronic toys (Rafferty and Hung, 2015). In the context of this paper, we refer smart toys as those who fall in the field of toy computing, which has an association between a physical toy and a mobile device and application.

By their nature, smart toys raise a different concern beyond child safety: security. Smart toys may manipulate confidential data such as private information and localisation, for example. In conventional systems, sometimes users may allow third parties to access their private information for marketing or customisation process. However, children are considered vulnerable users that may not make informed decisions about their own privacy policies.

Although parental control mechanisms, such as parents account and parents' consent interfaces, can mitigate relevant privacy issues, they aren't able to avoid attacks that compromise other security aspects, including information theft and denial of service.

In fact, several articles from relevant sources such as Forbes (Fox-Brewster, 2016), Fortune (Hackett,

Carvalho, L. and Eler, M.
Security Requirements for Smart Toys.
DOI: 10.5220/0006337001440154
In *Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS 2017) - Volume 2*, pages 144-154
ISBN: 978-989-758-248-6

2016) and PCWorld (Newman, 2015) have reported security flaws in smart toys. Such flaws range from private information leakages (bio information, photos) to outsiders interacting with children via a smart toy. This is a threat even to the children safety since they can provide confidential information and even unrestrictedly follow instructions given by the toy. Such a scenario raises an important question: how safe are the children around smart toys?

It is noticeable that there are only a few disclosed policies related to the security policies and requirements defined to address the issues related to smart toys. Generally, solutions are disclosed after a security flaw becomes public. Thus specific security policies and requirements must be considered in this scenario to assure the security of the information and even the safety of the children.

Mobile applications have been used for a long time in both personal and corporation environments, hence policies and requirements have been proposed to assure the security of mobile services and applications (Biswas, 2012) (Zapata et al., 2014) (Nagappan; 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.

The main difference between a typical mobile application and a smart toy is that the latter has 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. The fact that smart toys are basically used by children makes it even more challenging, since the security policies must comply with children rights and specific acts of each country or state.

This paper aims at analysing smart toys (or toy computing) from a security perspective to identify security requirements to mitigate the inherent security risks of this environment. We used a Security Requirements Engineering approach from Microsoft called Security Development Lifecycle (SDL) and a threat modelling tool to analyse the three components of a smart toy and their interaction. Accordingly, 15 threats and 20 security requirements have been identified and are presented.

The remainder of this paper is organised as follows. Section 2 shows the basic concepts of smart toys and toy computing. Section 3 presents the concepts related to security requirements. Section 4 discusses the related work. Section 5 presents the threats and the requirements identified as well the procedure used to identify them. Finally, concluding remarks and future directions are presented in Section 6.

2 SMART TOYS

Toys have been part of our culture for a long time as entertainment resources. According to specialists, they are essential for children cognitive, motor and social development. They are also used for educational and therapeutic purposes. The growing interest for technological gadgets from people of all ages has promoted the development of high tech toys, also known as smart toys.

Smart toys are 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.

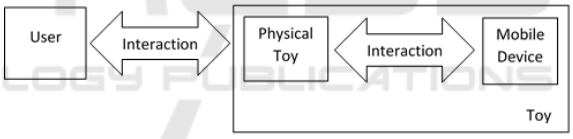

Figure 1: Toy computing environment.

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. Table 1 shows a comparison among traditional toys, electronic toys and smart toys.

2.1 Smart Toys Samples

There are few toys in the market that fit in the concept of toy computing. Amiibo refers to action figures of the famous characters of Nintendo video games such as, for example, Mario Bros and the Legend of Zelda. They use NFC technology to communicate with the consoles also built by Nintendo. Figure 2 presents an illustration of this smart toy. Among other features, one Amiibo allows the player to incorporate that character in a game, or

to use special features or receive a level upgrade, and so forth.

Table 1: Toys comparison.

	Traditional	Electronic	Smart
Interaction	Mechanical	Mechanical Sensor	Mechanical Sensor Visual Auditory Wireless
Data collection	No	Yes Limited	Yes
Data sharing	No	Yes Limited	Yes
Data storage	No	Yes Internal	Yes External
Processing capabilities	No	Yes Limited	Yes
Network capabilities	No	Yes Limited	Yes
Controlled by Mobile Devices	No	No	Yes

Note: Adapted from Rafferty and Hung (2015).

Figure 2: Super Mario Character Amiibo for Nintendo 3DS console (Adapted from www.nintendo.com).

Sphero has created a robotic ball, also called Sphero, that is controlled by a mobile application installed on a tablet or smartphone via Bluetooth. More than thirty applications are available for this toy. They allow users to use basic controls or create personalised programs to control the sphere.

The Tek Recon Hammer Head and Tech Recon Havoc are high performance blasters developed by Tech 4 Kids that along with a mobile device and a mobile application provide users with a realistic battle field game experience. Figure 3 presents the Havoc model of this smart toy. The mobile application uses the GPS technology provided by the mobile device to track the users in real time. It also allows users to communicate via voice message using Wi-Fi or 3G technology.

Figure 3: Tech Recon Havok (Adapted from www.tekrecon.com).

The Mattel Fisher-Price interactive learning smart toys with voice and image recognition features are capable to collect data to adapt to create personalized playing. Figure 4 shows the Smart Toy® Bear. Through the mobile app and a Wi-Fi connection, the smart toy gets updates and the parents can unlock bonus activities.

Figure 4: Smart Toy Bear (Adapted from http://fisher-price.mattel.com).

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.

My friend Cayla, a smart toy doll, and I-QUE Intelligent Robot, both from Genesis Toys, are smart toys able to answer several questions and, to improve user experience, connects to the Internet through a mobile device. Figure 5 shows I-QUE environment.

2.2 Some Smart Toy Security Flaws

Several mobile services, such as e-commerce, mobile banking and location-based services (Broll et al, 2007), use context data to provide customers with more personalized experiences. Examples of context data are age, sex, localisation, and so forth. Such information are usually stored in the mobile device and may be collected voluntarily, when the user informs personal data as required by the application; observed, when data is collected by the

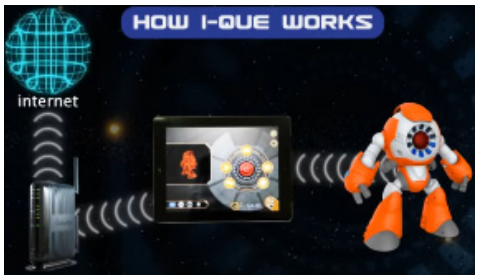

Figure 5: I-QUE Intelligent Robot (Adapted from http://ique-robot.co.uk/).

device's sensors; or inferred when some information is derived from the data observed or collected.

Likewise, most of the smart toys 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 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, for example.

Genesis Toys, which makes the Cayla and I-QUE products, 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. The Hello Barbie doll app, for example, could automatically connect to unsecured Wi-Fi networks and reveal confidential information (Newman, 2015). Some Internet servers may fail to authenticate users and expose data and profiles. A Smart Toy® Bear vulnerability in the backend systems enabled attackers to access private information.

As this specific market grows, so does the concerns around the security of smart toys, especially because they are massively used by children. Children are considered vulnerable and most of the times incapable of making informed or rational decisions, that is why they are usually covered by specific acts and children's rights depending on the country or state they live. In such a scenario, it is urgent a proper investigation of the possible threats and security requirements a smart toy should meet to assure a reasonable level of security for its users.

3 SECURITY REQUIREMENTS

Systems requirements are descriptions of the functionalities that a system must provide and its related constraints (Sommerville, 2011). They can be classified as functional requirements, when they refer to the features a system must have, usually related to business rules, and non-functional requirements, usually related to constraints over the systems functions such as Service Level Agreement (SLA), for example.

Security requirements aim at assuring the confidentiality, integrity and availability of a system, which are the fundamental principles behind information security along with privacy and non-repudiation. Security requirements are usually referred as non-functional requirements as they represent system constraints which may be implemented in many ways. For example, a redundant architecture to guarantee the availability of the system, or access control to assure confidentiality. But they may also be classified as functional requirements when they must provide authentication, for example.

For a long time, systems were developed almost exclusively to meet functional requirements and almost no attention was given to security requirements. Security issues were basically met by means of security patches released after the discovery of a vulnerability (Tondel et al., 2008). Nowadays, much more attention has been given to security requirements as the number of security incidents has been growing across the time. Figure 6 shows the number of security issues reported to the United States Federal Agencies (GAO, 2016).

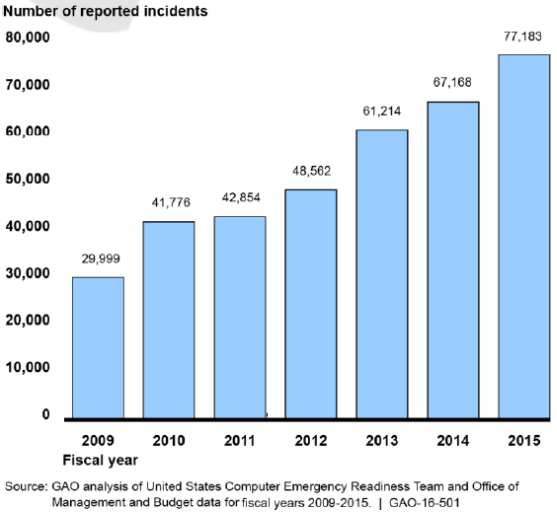

Figure 6: Security Incidents Report (GAO, 2016).

The process of identifying, analysing and documenting requirements is known as Requirements Engineering. Handling security requirements demands specific knowledge and practices, thus some authors classified the process of managing security requirements as Security Requirements Engineering (SRE). There are several SRE approaches found in the literature and used in industrial level, such as Comprehensive, Lightweight Application Security Process (CLASP), Security Quality Requirements Engineering (SQUARE), and the Security Development Lifecycle (SDL) from Microsoft, for example. Following, we present the details of such approaches.

3.1 CLASP

CLASP is composed of several security-related activities that can be integrated into any software development process, in order to build a security requirements set. Security requirements are formulated according to the following steps (Viega, 2004):

1. Identify system roles and resources.
2. Categorize resources into abstractions.
3. Identify resource interactions through the lifetime of the system.
4. For each category, specify mechanisms for addressing each core security services.

The requirements specifier, an important role in that process, is responsible for detailing security relevant business requirements, determining protection requirements for the architectural resources, and specifying misuse cases. Misuse cases describe actors' undesirable behaviour (Sindre; Opdahl, 2005).

The main activities related to requirements elicitation and performed by the requirements specifier are (Secure Software, 2005):

- Specify operational environment.
- Identify global security policy.
- Identify resources and trust boundaries.
- Detail misuse cases.

3.2 SQUARE

SQUARE is a process that aims to integrate security concerns into the systems development life cycle. This process consider nine steps in order to elicit, categorize and prioritize security requirements, as follow (Mead; Hough; Stehney, 2005):

1. Agree on definitions.
2. Identify security goals.
3. Develop artifacts to support security requirements definition.
4. Perform risk assessment.
5. Select elicitation techniques.
6. Elicit security requirements.
7. Categorize requirements as to level (system, software, etc.) and whether they are requirements or other kinds of constraints.
8. Prioritize requirements.
9. Requirements inspection.

The steps related to SRE are from 5 to 9, but the steps from 1 to 4 are very important to the success of this process (Mead, 2006). It is important to note that crucial artifacts, such as misuse case scenarios and diagrams, and attack trees, are created or assembled in the step 3 in order to assist the requirements elicitation process in the step 6. SQUARE can be used either to an under development system or to a released one.

3.3 SDL

Microsoft Trustworthy Computing SDL (Lipner, 2004) (Microsoft, 2011) stands for security software development and it has the main following phases and its security mandatory tasks:

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, unsecure 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 will occur in the first two phases. In the requirements 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.

During the design phase, performing a threat modeling is considered a critical activity, since it is a systematic process for identifying threats and vulnerabilities. The following steps are essential in threat modeling:

1. Diagram: system decomposition with Data Flow Diagrams (DFD).
2. Identify threats: system threat identification using the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege) approach.
3. Mitigate: address each threat identified.
4. Validate: validate the whole threat model.

Microsoft have developed the SDL Threat Modeling Tool to provide guidance on creating and analysing threat models.

4 RELATED WORKS

Ng and his colleagues (Ng et al., 2015), aware about security and privacy issues in the toys and mobile apps union, present in their work two main security and privacy concerns: location history and data tracking, and encryption and data security. Mobile devices connected to Internet through a mobile data plan or a Wi-Fi network are susceptible to different forms of attacks (denial of service, man in the middle, spoofing, etc.). These devices usually log location history that, when it is sent over the Internet, could be intercepted, exposing motion patterns and the real time individual location.

In order to provide security and privacy, the communications must use secure protocol to ensure identities and data encryption in the data exchange. Rafferty and her colleagues through a formal privacy threat model, developed by them and inspired by well-known threat modelling techniques, have investigated privacy requirements for toy computing (Rafferty et al., 2015). The analyses consider a threat architecture, illustrated in Figure 7, and they are performed in five (5) steps:

1. Architecture overview: architectural perspective of the toy computing application.
2. Assets and data flow: assets identification and application decomposition.
3. Privacy threats: privacy threats identification and mapping.
4. Methods of attack: privacy threat trees determination and misuse case scenarios creation.
5. Privacy requirements and Controls: privacy requirements and control proposal.

According to the toy computing nature and threat architecture, privacy are affected by the following:

- Child's Identity: identity is associated with collected data.
- Location Data: collection of location data and probably association with identities.
- Networking Capabilities: collected data sharing over a network.

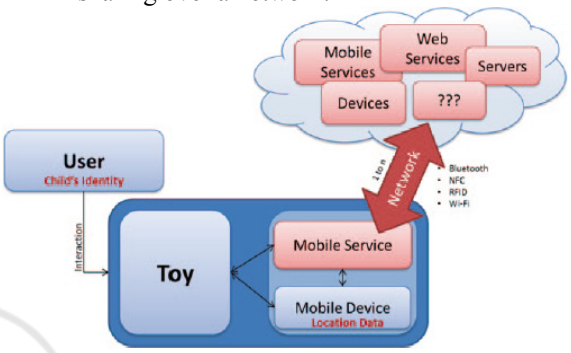

Figure 7: Threat Architecture (Rafferty et al., 2015).

As a result, they have compiled six (6) privacy rights (privacy requirements):

- The right for a parent/guardian to request restrictions on the use or disclosure of private information of their child.
- The right for a parent/guardian to access, copy, and inspect collected records on their child.
- The right for a parent/guardian to request deletion of their child's private data records, or correction if records are inaccurate.
- The right for a parent/guardian to request acknowledgements through a communication channel when private information of their child is collected.
- The right to file complaints to toy company.
- The right to find out where the child's private data has been shared for purposes other than a game.

Although these work addresses security issues for smart toys, they are restricted to privacy and confidentiality problems that, while very important, are not the only ones.

Rafferty and her colleagues 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., 2017).

5 SECURITY REQUIREMENTS FOR SMART TOYS

We used the phases Requirements and Design from the Microsoft SDL process in order to identify generic security requirements that could be used to develop any smart toy. We also used the threat modeling tool provided by Microsoft. We considered a typical toy computing environment in this analysis: a physical toy controlled by mobile applications running in mobile devices and using mobile services.

5.1 SDL Requirements Phase

During the Requirements phase, the main sources of information used to define the security requirements were laws and regulations the toy industry must comply with. As smart toys are massively used by children, the COPPA was also an important source of information. It defines, from the perspective of information security, the following issues regarding children information to be addressed:

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.

In general, personal and confidential information must be protected. Therefore, The Personal Information Protection and Electronic Documentation Act (PIPEDA) (Canadian Public Works and Government Services, 2000) was also considered during our analysis. It defines the following issues to be addressed:

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.

Although COPPA and PIPEDA cover many important security aspects, they may not be sufficient to meet all the requirements of all countries. Therefore, other security issues may arise from the analysis of specific rules and laws of some countries.

5.2 Design Phase

Based on the toy computing environment presented on Figure 1 and the threat architecture presented on Figure 7, the security analysis considered the context diagram (high level DFD) showed on Figure 8 and level 1 DFD showed on Figure 9.

In order to identify threats in this phase, we consider the main following assets:

- Physical toy.
- Mobile device.
- Mobile application (app).

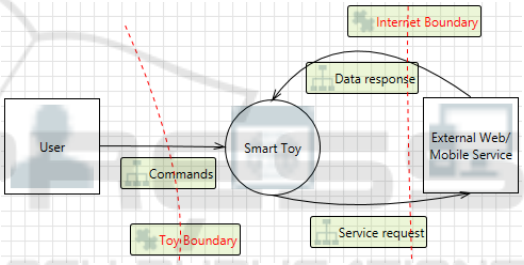

Figure 8: Toy Computing Context Diagram.

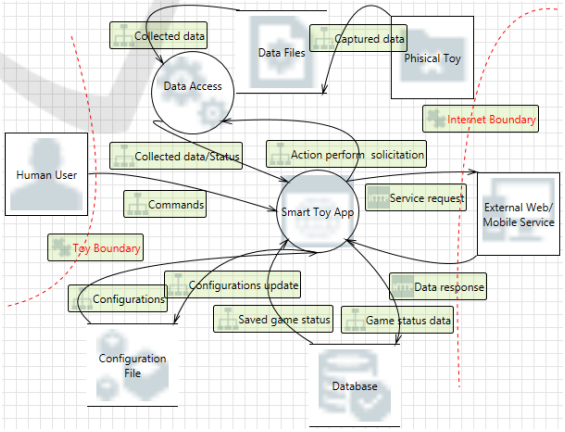

Figure 9: Level 1 Smart Toy Processes.

The mobile device through the mobile application collects, stores and shares data, therefore, we consider the following possible information assets:

- App database.
- Configuration files.

- Data files (location, images, video, audio, etc.).

The interaction between user, mobile device and physical toy exposes some system's entry points:

- Mobile app interface: user insert data into the mobile interface.
- Sensors of the mobile device: mobile device gets data by its sensors.
- Sensors of the physical toy: physical toy get data by its sensors.
- Communication between physical toy and mobile device: wireless network communication using local area network (LAN) or personal area network (PAN) protocols like Wi-Fi, Bluetooth, Near Field Communication (NFC), etc.
- Communication between mobile device and mobile service providers: wireless network communication using LAN and wide area network (WAN) protocols like Wi-Fi, 3G, 4G, etc.

5.3 Threats

The threats identified, through threat modeling technique supported by STRIDE are:

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. Modification of the configuration file of the mobile device (loads a configuration file not suitable for the user).
- T2.2. Modification of the information exchanged through network communication between the components (physical toy x mobile device x access point/router).
- T2.3. 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 (localisation, 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.

5.4 Security Requirements

Based on the results from the SDL's requirements and design phases, the minimum security requirements for smart toys in a toy computing environment that addresses the twelve raised issues and fifteen threats are:

SR1. The smart toy app must provide notice of what information it collects and the further use and disclosure practices.

SR2. 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.

SR3. The smart toy app must not ask for more personal information in order to continue its operation.

SR4. The smart toy app must authenticate users.

SR5. Communication between physical toy and mobile device must use a protocol that allow authentication and authorization mechanisms.

SR6. Mobile services providers must own digital certificates allowing identity verification.

SR7. Configuration file integrity must be maintained and verified in every mobile app play session.

SR8. Every communication in toy computing environment must use cryptographic mechanisms.

SR9. 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 nor 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 unnecessary personal information collected.

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

Table 2 presents which security requirement addresses witch security issues ant threats.

5.5 Results and Discussion

The twenty security requirements established in the section 5.4 address security concepts like confidentiality, integrity, availability, privacy, non-repudiation and authenticity. Most of the security issues are related to these six information critical characteristics.

It is possible to perceive the effectiveness of the security achieved when the proposed security requirements are met taking into account, for example, the recent security problems presented by the Smart Toy® Bear, Hello Barbie, Cayla and I-QUE Intelligent robot, all presented in the section 2.2 in this paper.

Table 2: Security Requirements versus Issues and Threats.

Security Requirement	Issues and/or Threats
SR1	I1 and I8
SR2	I2 and I8
SR3	I3
SR4	T1.1
SR5	I4, I12 and T1.2
SR6	I4, I5, I12, T1.3
SR7	I4, I12, T2.1
SR8	I4, I5, I6, I12 and T2.2
SR9	I4, I12 and T2.3
SR10	I4, I12 and T2.3
SR11	T3.1
SR12	I4, I6, I12 and T4.1
SR13	I4, I6, I12 and T4.2
SR14	I4, I12 and T4.3
SR15	I4 and T5.1
SR16	I4 and T5.2
SR17	I4, I6, I12, T6.1 and T6.2
SR18	I7 and I9
SR19	I10
SR20	I11

Security flaws in the Smart Toy® Bear caused by the use of unsecured application programming interfaces (APIs) (Hackett, 2016; Fox-Brewster, 2016) allowed attackers access personal information and send commands to the physical toy. These problems could be avoided by the implementation of the security requirements SR4, SR5, SR6, SR7, SR8, SR12, SR16 and SR17.

Several vulnerabilities was uncovered in the Hello Barbie doll like communications interception, personal information disclosure and connection to unsecured Wi-Fi network (Newman, 2015). These problems could be avoided by the implementation of the security requirements SR5, SR6, SR7, SR8, SR12 and SR17.

The Cayla doll and I-QUE Intelligent Robot, among other problems, allowed an attacker ask children personal information and unauthorized Bluetooth connections from any near mobile device (Baraniuk, 2016). These security issues are solved by the implementation of the security requirements SR3, SR4 and SR5.

The security requirements identified in this work cover the whole toy computing environment. Therefore, future advances in the development of smart toys that comply with this environment can also benefit from this list of security requirements. The results of this work can also serve as a basis for the elaboration of security policies, since toy manufacturers usually only have privacy policies, which are less comprehensive, besides evidencing the need to formally deal with information security,

which can be translated in the creation of future security standards to be met by the toy industry.

6 CONCLUSIONS

Computer systems have been a target of cybernetic attacks for a long time. Their association with traditional toys has created a new type of product called smart toy, which has also become a target for attackers. In this paper, we presented the main concepts and architectures behind this new environment called toy computing and we discussed the consequences of enlarging the attack surface by introducing a physical toy equipped with sensors and network communication and the vulnerabilities that might be exploited in this scenario. The security issue associated with the discussed scenario is aggravated by the fact that children are the main users of this technology and most of the time are not able to perceive situations of risk. We thus presented an analysis performed on the toy computing environment using the Microsoft SDL process and its threat modelling tool to identify the main vulnerabilities, threats and consequently the minimum security requirements that every smart toy must meet, so it does not expose its users to potentially harmful situations.

The identification of such security requirements is important to allow the developers to plan how the security mechanisms will be implemented during the development life cycle of the smart toys. As each new smart toy may have different characteristics and even electronic components, enlarging the surface attack and the potential threats, each new smart toy will require a proper security requirements elicitation and analysis in order to ensure that any new security requirements can be identified and later included in the general list of security requirements for smart toys. Moreover, the security requirements identified for toy computing can be used to derive security tests for toy computing considering all vulnerabilities and threats identified in different scenarios.

REFERENCES

Biswas, D., 2012. Privacy Policies Change Management for Smartphones. In *IEEE International Conference on Pervasive Computing and Communications Workshops,* pages 70-75.

Canadian Public Works and Government Services, 2000. Personal Information Protection and Electronic Documents Act.

Baraniuk, C., 2016. Call for privacy probes over Cayla doll and i-Que toys. BBC News, Technology, 6 Dec 2016. Accessed 12 Dec 2016, available at <http://www.bbc.com/news/technology-38222472>.

Broll, G., Hubmann, H., Prezerakos,G., Kapitsaki, G., Salsano, S., 2007. Modeling Context Information for Realizing Simple Mobile Services. In *Mobile and Wireless Communications Summit*, *2007. 16th IST*, pp. 1-5.

Deloite, 2015. Global Mobile Consumer Survey: US Edition - The rise of the always-connected consumer. Accessed 22 May 2016, available at <http:\\www.deloitte.com/us/mobileconsumer>.

Fox-Brewster, T., 2016. Hackers Could Have Turned Vulnerable Smart Teddy Bear Into Demon Toy. Forbes, Security, 2 Feb 2016. Accessed 08 Dec 2016, available at <http://www.forbes.com/sites/thomasbrewster/2016/02/02/fisher-price-hero-vulnerable-to-hackers/#359130c71cfe>

GAO, 2016. United States Government Accountability Office. Information Security – Agencies Need to Improve Controls over Selected High-Impact Systems, GAO-16-501. Accessed 24 May 2016, available at <http://www.gao.gov/assets/680/677293.pdf>

Hackett, R., 2016. This FisherPrice Smart Toy Bear Had Data-Leak Vulnerability. Fortune, Tech Internet of Things, 2 Feb 2016. Accessed 08 Dec 2016, available at < http://fortune.com/2016/02/02/fisher-price-smart-toy-bear-data-leak/>

Lipner, S., 2004. The Trustworthy Computing Security Development Lifecycle. Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04), IEEE.

Mead, N., 2006. SQUARE Process. The Build Security In. Software Engineering Institute, Carnegie Mellon University. Accessed 03 Nov 2016, available at <https://www.us-cert.gov/bsi/articles/best-practices/requirements-engineering/square-process>.

Mead, N., Hough, E., Stehney, T., 2005. Security Quality Requirements Engineering (SQUARE) Methodology. CMU/SEI-2005-TR-009, Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

Microsoft, 2011. Security Development Lifecycle, SDL Process Guidance. Version 5.1, April 14. Accessed 24 Feb 2017, available at <http://www.microsoft.com/sdl.>

Nagappan, M., Shihab, E., 2016. Future Trends in Software Engineering Research for Mobile Apps. In *IEEE 23rd International Conference on Software Analysis, Evolution, and Reengineering (SANER), Volume 5,* pages 21-32.

Newman, J. 2015. Internet-connected Hello Barbie doll can be hacked. PCWorld, Security, News, 7 Dec 2015. Accessed 12 Dec 2016, available at <http://www.pcworld.com/article/3012220/security/internet-connected-hello-barbie-doll-can-be-hacked.html>

Ng, M., Chow, M., Salgado, A., 2015. Toys and Mobile Applications: Current Trends and Related Privacy Issues. Mobile Services for Toy Computing.

International Series on Computer Entertainment and Media Technology, Springer, 2015, p. 51-76. ISSN 2364-947X.

Rafferty, L.; Hung, P., 2015. Introduction to Toy Computing. Mobile Services for Toy Computing. International Series on Computer Entertainment and Media Technology, Springer, 2015, p. 1-7. ISSN 2364-947X.

Rafferty, L., Fantinato, M., Hung, P., 2015. Privacy Requirements in Toy Computing. Mobile Services for Toy Computing. International Series on Computer Entertainment and Media Technology, Springer, 2015, p. 141-173. ISSN 2364-947X.

Rafferty, L., Hung, P., Fantinato, M., Peres, S., Iqbal, F., Kuo, S., Huang, S., 2017. Towards a Privacy Rule Conceptual Model for Smart Toys. In *Proceedings of the 50th Hawaii International Conference on System Sciences*, *HICSS*, Jan 04.

Secure Software, 2005. The CLASP Application Security Process. Secure Software, Inc. Accessed 16 Nov 2016, available at <https://www.ida.liu.se/~TDDC90/literature/papers/clasp_external.pdf>.

Sindre, G., Opdahl, A., 2005. Eliciting Security Requirements with Misuse Cases. *Requirements Eng*., vol. 10, no. 1, pp. 34–44.

Sommerville, I., 2011. Software Engineering. 9th Edition, Pearson Education.

Tondel, I., Jaatun, M., Meland, P., 2008. Security Requirements for the Rest of Us: A Survey. IEEE Software, vol. 25, Issue No. 1 – January/February.

United States Federal Trade Commission, 1998. Children's Online Privacy Protection Act of 1998. Accessed 27 Nov 2016, available at <http://www.coppa.org/coppa.htm>.

Viega, J., 2005. Building Security Requirements with CLASP. In *Proceedings of the 2005 Workshop on Software Engineering for Secure Systems & Mdash, SESS'05*, May 15-16, St. Louis, MO, USA.

Zapata, B., Niñirola, A., Fernández-Alemán, J., Toval, A., 2014. Assessing the Privacy Policies in Mobile Personal Health Records. In *36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 4956-4959.