Tendencias en seguridad

Methodology to Securitize Smart Toys in Household Environments

P. González, F. Paniagua, D. Suárez and J. J. Nombela

Resumen — **This paper examines the present situation regarding Smart Toys, the privacy and security concerns that they generate for children and their relatives, as well as the existing solutions that would allow them to improve the security of these devices. On this purpose, it is examined the state of art in this field, including some recent data breaches concerning Smart Toys, and the present available solutions to identify and mitigate their security risks. As a result of not identifying a suitable methodology that provides a unified approach to analyze and securitize household environments composed by different Smart Toys that can easily be implemented by non-technical users, in this paper is proposed a new and tailored methodology. The presented proposal aims to tackle and solve the identified security concerns and present the information in a user-friendly manner, helping final users to understand and address the security issues of their Smart Toys, even without having a deep technical knowledge in the field.**

Palabras clave — **Methodology, Security and Privacy Protection, Risk Management, Internet of Things, Smart Toys.**

I. INTRODUCTION

THE NUMBER of IoT devices and services which are being used nowadays has been experimenting an exponential growth for the past ten years. A ccording to Gartner's predictions, it is expected that by 2020 the number of connected devices will reach the 20 billion [1], and other sources, such as Mozilla, share even more ambitious figures [2].

Along with the increase of the number of devices in use there is also an important expansion of the vulnerability surface for these devices and the number of threats they are exposed to. This situation is also concerning to Smart Toys users, which showed on an ESET survey that more than one third of them are very worried about the privacy and security of children using these devices [3].

Bearing this in mind, it was conducted a deep research on the existing solutions that could allow users to identify the threats and risks surrounding the Smart Toys they possess, as well as the security measures that could be implemented to mitigate the identified risks.

As a result, several security risk methodologies, frameworks and guidelines were analyzed, but most of them were hardly adapted to such a specific IoT environment. On top, most of the identified resources were targeted to an audience with a reasonable level of technological understanding, which is why they could not be implemented by the average users of Smart Toys (children and/or parents).

These circumstances lead to a complex situation: the users of Smart Toys not only ignore the risks they are exposing their families to, but in case of having interest in securitizing their IoT environment, they cannot rely on a user-friendly procedure or reference that helps them to accomplish this mission [4].

Thus, this paper analyzes the present situation of Smart Toys, the threats that can affect them, and the methodologies that could be used as a reference to securitize IoT environments. Also, and due to the deficiencies of the existing methodologies to solve the aforementioned problems, it is proposed a methodology that allows users to identify, understand and take decisions about the security settings of their Smart Toys.

The methodology proposed is also validated, using a real case of a Smart Toy data breach, to verify that it can actually contribute in identifying the risks these toys can expose users to, improving their knowledge and understanding of them. Moreover, it can also be used as a reference for developing a security framework that can be used to identify risks and mitigations of household I oT devices, or even other kind of environments with similar features.

The rest of the paper is organized as follows. Section 2 presents briefly an overview of the IoT architectures and security. Section 3 analyzes the security gaps for Smart Toys. Section 4 describes the proposed methodology. Section 5 tests and validates the proposed methodology. Section 6 presents some conclusions extracted from the work carried out in this paper.

II. CONTEXT AND STATE OF THE ART

Definition of Smart Toys

To understand what a Smart Toy makes reference to, it is important to first understand what the concept IoT (Internet of Things) stands for.

Even though there is not an official definition of the term yet, if we consider the definitions provided by reference institutions such as the IEEE [5], ENISA [6] or Gartner [7], there is certain conseus agreeing that the term IoT comprises a wide ecosystem of interconnected services and devices.

The Smart Toys are just a specific type of IoT that are intended to interact with children and their environment as part of a leisure activity.

P. González, Universidad Internacional de La Rioja, Madrid, Spain, paulagonzalezdom@gmail.com

F. Paniagua, Universidad Carlos III, Madrid, Spain, fidel.paniagua@uc3m.es

D. Suárez, Universidad Internacional de La Rioja, Madrid, Spain, diego.suarez@unir.net

J. J. Nombela, Universidad Internacional de La Rioja, Madrid, Spain, juanjose.nombela@unir.net

Corresponding author: Fidel Paniagua Diez

https://doi.org/10.12804/si9789587844337.07

IoT Architectures

Likewise it happens with the definition of the term, there is not a standard model or architecture for IoT environments, and the proposals varie depending on the source consulted.

In broad strokes the architecture of an IoT environment can be represented by three, four or five layers [8], to understand the main interactions among all the involved devices:

(i) *Three Layer Architecture*: Differentiates between the Perception Layer (to identify and collect information), the the Network Layer (to transmit data between layers) and the Application Layer (defines the applications related to the IoT).

(ii) *Four Layers Architecture*: Apart from the previous layers, it also considers a Support Layer, which contains the security implementations.

(iii) *Five Layers Architecture*: Considers the three first layers, named the Perception, Transport and Application layers, and two more layers, which are the Processing Layer (middleware layer that processes the collected information) and the Business Layer (allows the management of the whole IoT system).

Apart from the generic architectures mentioned above, there are further architecture models that renowned institutions, such as Gartner, propose, such as their Reference Model composed by five layers (Process, Function, Information, Communication and Device) and three tiers (Edge, Platform and Enterprise) [7].

Available Security Solutions

As it has been shown, understanding and analyzing IoT environments can be a challenging task, due to the general lack of consensous. This is an important handicap when the Smart Toys, or IoT in general, are studied from a security point of view.

Nowadays, there are several institutions working towards improving the security of IoT environments. Concerning children data privacy there are two main regulations around the world that are having a great impact in this context:

(i) *COPPA (Children's Online Privacy Protection Act)*: In the United States of America, this regulation defines certain requirements that operators of websites and online services must consider when their services are directed to children under 13 or when they are collecting personal information of them [9].

(ii) *GDPR (General Data Protection Regulation)*: This regulation defines a common data protection frame in Europe, imposing great sanctions to data processors and controllers that do not use are not implementing suitable security measures for the data they are processing [10].

There are also institutions that, even if they do not have a legal influence over the design or production Smart Toys, are developing resources such as guides, methodologies or frameworks to improve the overall security of IoT environments; some of them have even make some contributions to the specific field of Smart Toys, providing generic guidelines showing the basic steps to improve the security of a Smart Toy [11]. However, the overall maturity level of the field, in terms of standardization, is still low.

Some of the most representative contributions in this field are the following ones:

(i) *OWASP IoT Project*: In 2015 the Open Web Application Security Project presented a draft about the attack surface areas and security considerations for IoTs [12].

(ii) *European Union Agency for Network and Information Security (ENISA)*: In 2017 ENISA published a study titled '*Baseline Security Recommendations for Internet of Things in the context of critical information infrastructures*', which aims to set the scene for IoT security in Europe, providing insight into the security requirements of IoT, mapping critical assets and relevant threats, assessing possible attacks and identifying potential good practices and security measures to apply in order to protect IoT systems. It serves as a reference point in this field and as a foundation for relevant forthcoming initiatives and developments [6].

(iii) *National Institute of Standards and Technology (NIST)*: In February of 2018 the '*NIST Internal Report*' (NISTIR) published a draft for IoT security, that aims to inform and enable policymakers, managers, and standards participants as they seek timely development of and use of cybersecurity standards in IoT components, systems, and services. It brings a good frame to understand the cybersecurity landscape for IoT and identify the areas where security standards are missing, but it does not provide yet a security framework itself [13].

(iv) *Gartner*: In 2018, the Gartner Advisory Company released the already mentioned paper called '*Architect IoT Using the Gartner Reference Model*' which provides an architecture blueprint that defines what functionality is required, where that functionality will operate, and how data and control will flow in an IoT project [7].

(v) *Microsoft*: In 2018 Microsoft Azure published a Security Architecture for IoTs that through a Threat Model defines a path to identify security threats in very diverse contexts [14].

Even though all the abovementioned efforts contribute with very interesting insights into the field of study, there are still important security issues that are not addressed or solved by these proposals, leaving children and their relatives totally exposed to data breaches and other security and safety risks of Smart Toys.

III. SECURITY ANALYSIS

Security Breaches for Smart Toys

Within the past years, there have been several security breaches concerning Smart Toys which have compromised the Privacy and Security of the children using it, as well as their own Safety and of the ones surrounding them. The much talked-about are the following:

(i) *VTech*: The company VTech sells toys and gadgets for children, including tablets, phones and baby monitors. In November 2015, it was announced that a security breach had occurred and that it exposed personal information and photos of almost 5 million parents and more than 6 million kids due to bad security practices (weak encryption algorythms or lack of them, passwords stored in plain text, vulnerabilities to SQL injections, etc) [15].

(ii) *CloudPets*: The Smart Toy allowed children to send and receive audio recordings between them and an external app that can be installed in most of the smartphones and tablets of the children's relatives. At the beginning of 2017 an important leakage of 820,000 user accounts was reported, which included the personal information, photos and recordings mainly of children, but also of their families, mainly on account of the data storing and the production website were publicly facing a network segment without any authentication or password required, apart from other security misconfigurations [16] [17].

Apart from the above metioned ones, there are some other examples that also show not only the consequences to Smart Toy security breaches, but also the risk potential that these devices have, as well as the general perception of customers about them. Some of the following are very representative:

(i) *Hello Barbie*: By the end of 2015, the toy company Mattel and the technology company ToyTalk announced the launch of a Smart Barbie called '*Hello Barbie*'. Apart from collecting data, the Hello Barbie owed an Artificial Intelligence (AI) and a voice recognition software that allowed the toy to have very realistic conversations with the children and adapt her answers. Many concerns were raised when the company stated that the voice-recordings would be shared with third parties to improve the experience of the users, which lead to a public petition with more than 37,000 signatures to drop the toy from the market [18].

(ii) *My Friend Cayla and i-Que Robot*: Another two Smart Toys based on AI called '*My Friend Cayla*' and '*i-Que Robot*', launched by the company Genesis Toys in collaboration with ToyQuest and Nuance Communications, had a very bad reception from the parents and even federal institutions on their latest release by the end of 2016. The allegations were based on the poor security features of the doll and the position of the company about sharing data with third parties [19].

Apart from the present field of study (Smart Toys), there are other IoT devices that can interact with these devices or their targeted users, such as Echo devices, which have also brought to attention security concerns that should be addressed. A well know n example is the case of a six years old kid who buyed a dollhouse just by ordering it to the Echo device [20].

Gaps in the Existing Security Solutions

The just-mentioned security breaches have occurred and impacted data subjects despite the previously mentioned existing security solutions. This happened because of the also mentioned security gaps surrounding these solutions. As a summary, can be pointed out the following three main problems:

(i) *Lack of agreement on the considerations*: The lack of consensous concerning all the IoT world generates a lot of doubts about which procedure to follow to identify security risks and mitigations for Smart Toys. Moreover, some of the mentioned methodologies are too specific for the environments they have been designed for, not allowing the flexibility of implementing them for this specific use case.

(ii) *The implementation procedure is not clear*: Aligned with the previous point, even though the regulations and frameworks help to promote a security culture among Smart Toy manufaturers, they refer to what should be considered but not how to implement their requirements on products and services.

(iii) *Language and approach*: Most of the available solutions are oriented to a target audience that can interfere at the first stages of the commercialization of a Smart Toy (suchs as manufacterers or intermediates), which most likely will have certain technical knowledge. However, when these agents fail to provide the pertinent security to their products and services, final users are very vulnerable to security breaches. Most of them are not aware of the security risks their use can imply, or, even in the case of being interested, the available sources or information are not addressed in a user-friendly language, hindering their ability to interfere in the management of the IoT security.

Apart from these main problems, there are also other additional considerations that should not be forgotten, such as the diversity of features and elements that can comprise each Smart Toy or IoT system (different communication protocols, software features, etc.), or the wide assortment of vendors, functions and outcomes for every new toy that is introduced in the market.

IV. METHODOLOGY PROPOSAL

This paper proposes a modular security methodology that can be used in different household environments with different Smart Toys. The principal focus is to cover the security gaps previously identified and to develop a security methodology that allows the identification of Smart Toys security risks and mitigations, in a flexible, but still complete way.

It consists on a set of six defined steps which are the following:

(i) *First Step*: Delimitation of the Environment

(ii) *Second Step*: Identification of the Roles Involved

(iii) *Third Step*: Identification of the Technologies Involved

(iv) *Fourth Step*: Identification of the Functions for each Technology

(v) *Fifth Step*: Identification of the Security Risks for each Function

(vi) *Sixth Step*: Identification of Mitigations for each Risk

Each one of these steps will be explained in detail in the following sections.

First Step: Delimitation of the Environment

The first step consists in the definition and delimitation of the physical and virtual space that composes the Smart Toy environment.

Using as a reference the already mentioned architectures and methodology sources, in this paper is proposed a simplified architecture for a household setting, to contextualize the environment where the Smart Toys are located. The main elements contained would be the following:

(i) *Edge Devices (Smart Toys)*: It refers to the virtual and physical elements that integrate the IoT ecosystem.

(ii) *Edge Computing*: It refers to a distributed IT architecture, in which user data are collected, stored, exchanged and processed at the periphery of the network, but still close to the original source of the data. This allows the processing of time-sensitive data in almost real time, avoiding also the time lapse and costs derived from Cloud Computing.
(iii) *Edge Gateway*: It refers to the physical or virtual node that serves as the connection point between different Edge Devices, as well as between the IoT ecosystem and outsider networks. It provides system interoperability, communication and data-processing capabilities, among other features.
(iv) *Cloud Computing*: It refers to the use of remote services such as software, platforms or infrastructure, to store, process and retrieve data from an off-site location. In the IoT context it is generally used for historical analysis, big data analytics and long-term storage.
(v) *Cloud Backend*: It refers to the server side on a Cloud Computing service where all the processes actually take place.

As it is shown, the environment comprises not only the physical space where the devices are allocated, but also the area of influence of the communications among devices and their connections with external parties. On this purpose, it is important to list the elements present in the space but also to represent them graphically to better understand their connections and interactions.

Second Step: Identification of the Roles Involved

The second step consists in the identification of all the roles that can interact or influence the IoT ecosystem. The role is a representation of one or several natural or legal people, that share some common particularities.

Considering the kind of actors that can interact with the Smart Toy environment, in this paper are proposed three main categories of roles with similar features:
(i) *Users*: Commonly with low cybersecurity knowledge, access to security solutions and almost no influence on the technical design and features of the devices
(ii) *Authorized third parties*: such as the producers or service provides, which commonly prioritize commercial features instead of security ones.
(iii) *Unauthorized third parties*: such as intruders or unintended natural or legal persons which can interact with the Smart Toys.

This classification is important to understand who can influence the security of the IoT ecosystem, either through the improvement of it or through the generation of risky situations.

Therefore, depending on the focus of interest while implementing this methodology, it will be more or less interesting to also include certain level of granularity on the classification, instead of using the three previously-defined categories of roles for a household environment. The level of granularity can especially be affected depending on who is implementing the methodology, and which are the specific purposed for its implementation.

Third Step: Identification of the Technologies Involved

The third step consists in the identification of all the technologies involved in the IoT ecosystem.

Considering all the sources mentioned in the research analysis, but in particular ENISA [6] and Gartner [7], in this paper is proposed the following classification:
(i) The main devices should have the the following IoT features:
- *Tags* (to identify the device)
- *Sensors* (capacity that allows to collect data)
- *Communicators* (to transfer the data)
- *Actuators* (to take actions depending on the processing of the data)
- *Software/Hardware* (to be able to perform and support the processing operations)

(ii) Peripherical elements that can interact with the main device:
- *Physical devices* (e.g. remote controls)
- *Software elements* (e.g. applications)
- *Elements of the IoT network* (e.g. routers or gateways)

This identification and classification should be assigned to each of the IoT items composing the IoT environment.

Fourth Step: Identification of the Functions for each Technology

The fourth step consists in the identification of all the functions that each of the previously identified technologies possess.

Based on the existing researches in the field, in this paper are proposed a group of six main functions that a Smart Toy could perform, regarding to data processing:
(i) *Data Collection*: This function is carried out mainly by the sensors. They can detect changes in a physical or virtual level.
(ii) *Data Storing*: The data gathered by the sensors or provided by other IoT elements can be stored temporarily or permanently at the edge and/or at the cloud.
(iii) *Data Analysis*: The data gathered can be manipulated in order to obtain information that can be used by the IoT and provide a specific output in a timely manner. Common manipulations are the aggregation, organization, transformation or even deletion of data, to allow a faster and more efficient processing of the data gathered.
(iv) *Data Transmission*: The data can be transmitted to peripherical elements using wired or wireless communication technologies.
(v) *Data Display*: The data gathered and processed allows the IoT actuators and interfaces to show or display specific behaviors, that can cause a physical and/or a digital impact.
(vi) *Data Management*: This concept comprises the ability of influencing data to take decisions over all the previous functions, as well as about aspects such as the purpose of the data processing, the access and security of this data, among other functional decisions.

To be able to trace the steps, it is recommended to design a table, a tree diagram, or a similar structure, that allows to link each function to each of the identified technology, while it also provides a visual representation of where the most sensitive areas of the IoT can be located.

Fifth Step: Identification of the Security Risks for each Function

The fifth step consists in the identification of security risks associated to each of the functions previously defined, as well as which of the studied roles can cause each risk.

Consequently, at this point is necessary not to only identify the set of risks affecting the Smart Toy environment, but also to correlate each of them with the roles identified in previous steps. It is suggested to continue with the representation previously chosen (table, chart, etc.), allowing an easy correlation between the function of each technology and its correspondent risk.

Regarding to the correlation of each risk with the role generating it, would be as simple as to include another section (column, brunch, etc.) in the chosen representation, where this role is indicated following the previous classification. In Table 1 are described the most common correlations:

TABLE 1
RISK-ROLES CORRELATION

ROLE	R/R ID	ORIGIN
Provider	PR1	Poor security design of the IoT architecture
	PR2	Misuse of data from this party
User	UR1	Poor choice of the security configurations or actions
	UR2	Misuse of the device or system

As a consequence, unauthorized third parties could intrude or affect the IoT systems endangering their confidentiality, integrity or availability and its related roles.

In the Table 2 has been developed a high level classification of security risks that can affect IoT environments.

TABLE 2
RISK-FUNCTIONS CORRELATION

FUNCTIONS	RISK ID	DEFINITION
Data Collection	CR1	The information is not collected or is not accurate
	CR2	Unauthorized information is collected
Data Storing	SR1	If the databases are not secured, the collected data can be accessed or tampered
	SR2	If there is no backup of the information, it can be lost
Data Analysis	AR1	If the software is tampered or misconfigured, the results of the data analysis could not be the intended ones
	AR2	If the data provided is not essential to carry out the main activity of the device, could be used for illegitimate purposes
	AR3	Depending on the data provided, could be used for profiling
Data Transmission	TR1	If someone is located in the transmission area, can eavesdrop or tamper the data collected or displayed
	TR2	If the transmission is not encrypted, it can be eavesdropped or tampered
	TR3	If someone interferes the connection, can eavesdrop or tamper the data collected or displayed Data Display
Data Display	DR1	Legitimate information is not displayed
	DR2	Tampered information is displayed
Data Management	MR1	If there is no access control or it is inadequate, unauthorized users can access the device and its features
	MR2	If there is no authentication control or it is inadequate, unauthorized users can impersonate legitimate ones
	MR3	If there are no lost access procedures, or they are inadequate, legitimate users could lose access to the services provided
	MR4	If there are no update measures or they are inadequate, security vulnerabilities could not be patched
	MR5	If the password policies are not strong enough, unauthorized users can impersonate legitimate ones
	MR6	If the application has not been securely developed, data can be accessed or tampered

Even though the list provided is not exhaustive, in conjunction with the rest of identified elements, can provide a clear picture about the origin and impact of the security risks. Moreover, this classification can also be complemented with Information Security generic risks, which can be obtained from risks or threats catalogues such as the ENISA Threat Taxonomy [6].

Sixth Step: Identification of Mitigations for each Risk

The sixth step consists in the identification of mitigations that can be implemented to reduce or even eliminate the risks associated to the functions of each technology that composes the Smart Toys ecosystem, as well as which of the studied roles can mitigate that risk.

Consequently, as in the previous step, it is necessary to identify the set of mitigations for each identified risk, and to correlate it with the role that can implement the suggested mitigation. Likewise, it is suggested to continue with the previously chosen representation (table, chart, etc.) and proceed like it is described on the step 5.

Regarding to the correlation of each mitigation with the role generating it, the most common correlations would be the ones described in Table 3:

TABLE 3
MITIGATION-ROLES CORRELATION

ROLE	R/M ID	MITIGATION
Provider	PM1	Can only be implemented by design and before the IoT is distributed
	PM2	Can be implemented remotely and once the IoT is already operating
User	UM1	Can alter the security configurations of the IoT to mitigate the risk
	UM2	Cannot mitigate the risk, meaning that it is necessary to decide whether accepting the risk or rejecting the use of the IoT

In the same way that it happened in the previous step, the identification of security mitigations is also too broad to be tackled in the present project. For this reason, in Table 4 are only represented the main identified mitigations for the previously described risks. Moreover, the technical implementation of each of these mitigations will also depend on the choice of th e implementor and the available resources for this purpose.

TABLE 4
RISK-MITIGATIONS CORRELATION

FUNCTION	RISK ID	MIT. ID	MITIGATION DESCRIPTION
Data Collection	CR1	CM1.1	To include an informing feature when the information is properly collected
		CM1.2	To include integrity solutions, such as hashing or certificates
	CR2	CM2	To include an information-restricted configuration, attending to the principle of Need-to-know.
Data Storing	SR1	SM1	If the storing service is outsourced, only use trusted vendors and solutions
	SR2	SM2	To define backup solutions or infrastructures
Data Analysis	AR1	AM1	To require and provide only the essential information to carry out the expected service.
	AR2	AM2	To require and provide only the essential information to carry out the expected service.
	AR3	AM3	To require and provide only the essential information to carry out the expected service.
Data Transmission	TR1	TM1.1	To monitor all the connections stablished
		TM1.2	To activate diode functionalities (only entrance/only release)
	TR2	TM2.1	To enable and use secure transmission protocols
		TM2.2	To include integrity solutions, such as hashing or certificates
	TR3	TM3.1	To monitor all the connections stablished
		TM3.2	To enable and use secure transmission protocols
		TM3.3	To close unused ports
		TM3.4	To activate diode functionalities (only entrance/only release)
Data Display	DR1	DM1	To include an informing feature when the information is displayed, or it fails to be displayed
	DR2	DM2	To include integrity solutions, such as hashing or certificates
Data Management	MR1	MM1.1	To include access control features
		MM1.2	To use the principle of Need-to-know
	MR2	MM2.1	To provide solid authentication control features
		MM2.2	To use hardened passwords, codes or methods of authentication to avoid impersonation based on easy-to-access private data of the user
	MR3	MM3.1	To use hardened lost access procedures control
		MM3.2	To avoid the use of unreasonable requirements for access control in non-critical cases, that would lead the user to easily lose or forget the access credentials
	MR4	MM4.1	To provide means of update for devices and services
		MM4.2	To verify the software keeps updated with the last released versions
	MR5	MM5.1	To guarantee hardened password policies
		MM5.2	To avoid unsecure

			practices such as the reuse of passwords or the use of data easy to guess or to obtain
	MR6	MM6.1	To guarantee S-SDLC practices
		MM6.2	To only use applications and devices provided by trusted vendors

The provided list can also be used as a base for future studies, where it can also be completed and updated accordingly to the evolution of the currently studied IoT field.

V. VALIDATION OF THE METHODOLOGY

To test if the proposed methodology can successfully achieve the goal it has been designed for, it is layed out a real scenario with the CloudPet Smart Toy. This has been the toy of choice due to the great number of vulnerabilities identified that lead to its previously mentioned data breach [16 [17].

The proposed methodology defines a process step by step which allows to identify and map the features of the toy with all the described elements, resu lting in the identification of risks for the toy, as well as the roles generating them. The output of it is shown in Table 5.

TABLE 5
CLOUDPETS RISKS IDENTIFICATIONS

ASSETS	TECHN.	FUNCTIONS	RISKS	ROLES
Main Device	Sound Processor	D. Display	DR2	PR1
	Bluetooth LE	D. Transmission	TR1, TR2, TR3	PR1, UR2
	Wi-Fi	D. Transmission	TR2, TR3	PR1, UR1, UR2
Periph. Elements	Web App	D. Analysis	AR2	PR1, PR2
		D. Storing	SR1	PR1
		D. Management	MR, MR4, MR6	PR1
			MR2	UR2
			MR5	PR1, UR1
	Mobile App	D. Management	MR1, MR4, MR6	PR1
			MR2	UR1
			MR5	PR1, UR1
		D. Collection	CR2	PR1, UR1, UR2
		D. Display	DR2	PR1

Considering the risks identified by the methodology and the ones pointed out by prestigious security professionals such as Troy Hunt [16]or Paul Stone [17], it can be seen that they are actually aligned.

Once the risks have been identified, it is also possible toidentify the security mitigations that would be related to each of the identified risks, as it is shown in Table 6.

TABLE 6
CLOUDPETS RISK MITIGATIONS

RISKS ID	MIT. ID	IDENTIFIED MITIGATION	ROLES
SR1	SM1	If the storing service is outsourced, only use trusted vendors and solutions	PM1, PM2, UM1
AR2	AM2	To require and provide only the essential information to carry out the expected service.	PM1, PM2, UM1
TR1	TM1.1	To monitor all the connections stablished	UM1
	TM1.2	To activate diode functionalities (only entrance/only release)	PM1, PM2, UM1
TR2	TM2.1	To enable and use secure transmission protocols	PM1, UM1
	TM2.2	To include integrity solutions, such as hashing or certificates	PM1, PM2
TR3	TM3.1	To monitor all the connections stablished	UM1
	TM3.2	To enable and use secure transmission protocols	PM1, PM2, UM1
	TM3.3	To close unused ports	PM2, UM1
	TM3.4	To activate diode functionalities (only entrance/only release)	PM1, PM2, UM1
DR2	DM2	To include integrity solutions, such as hashing or certificates	PM1, PM2
MR1	MM1.1	To include access control features	PM1, PM2
	MM1.2	To use the principle of Need-to-know	PM2
MR2	MM2.1	To provide solid authentication control features	PM1, PM2
	MM2.2	To use hardened passwords, codes or methods of authentication to avoid impersonation based on easy-to-access private data of the user	PM1
MR4	MM4.1	To provide means of update for devices and services	PM1, PM2, UM1
MR5	MM5.1	To guarantee hardened password policies	PM1, PM2

	MM5.2	To avoid unsecure practices such as the reuse of passwords or the use of data easy to guess or to obtain	PM2, UM1
MR6	MM6.1	To guarantee S-SDLC practices	PM1, PM2
	MM6.2	To only use applications and devices provided by trusted vendors	PM1, UM2

As a consequence, there can be extracted the following conclusions:

- The methodology outcomes are aligned with the criterias and analysis of security experts, what shows that its results are reliable.

- It provides a clear context, common for any IoT environment, and an approach enough flexible to be able to be adapted to any Smart Toy use case, addressing the lack of agreement gap.

- It provides a well structured step by step procedure, that shows exactly what to consider, but also how to implement it, solving the concerns about the unclear implementation procedures.

- The language is simple and easy to understand, even by users with no deep technical knowledge. However, there is an important nuance that should be considered regarding this last point: the person implementing the methodology has to know perfectly which are th e technical features and functions of the toy, to identify their risks and if they have already been mitigated by the manufacturer or not.

If that would not be the case, the subject would have two options to tackle this issue: consulting the instructions or manufacturing features of the toy (in its own packaging or on the internet, for example) until gathering enough information, or using a supporting tool that automates the analysis process.

On this behalf, a proposal would be to automate the execution of the methodology, including the elements scan, on a device with which the users can interact, such as a gateway. This device, through questions or text options, would guide the process and automatically perform the risk assessment, showing the users the resulting information and/or mitigations for the scanned Smart Toys vulnerabilities.

In this case, through a user-friendly interface, the device would manage itself the most technical-related steps and would allow the users to be informed, interact and decide about the IoT systems in a simple and intuitive manner. This would allow users to manipulate configurations and harden their Smart Toys, whenever this would be possible.

As well, in the cases that scape to the user control, it would at least inform them about the risks they may be taking in a simple language, allowing them to take in-formed decisions about their choices of using or not certain Smart Toys.

VI. CONCLUSIONS

Main Contributions

After the present research and development, there could be extracted the following conclusions:

(i) The proposed methodology addresses a current problematic existing in the IoT, and more particularly, Smart Toy industry, covering the security gaps of other existing security solutions.

(ii) It gathers all the key aspects that should be considered while identifying security risks in Smart Toys environments through an approach enough flexible to consider different types of Smart Toys, but also enough defined to be accurate on the results provided.

(iii) It also defines a security framework for a specific IoT environment that can be used as a base in further studies to develop a scalable or more detailed methodology to securitize other IoT environments.

(iv) Its flexible approach and high level of definition also provide the ability to adapt the implementation of it depending on the target audience for its use, which can be particularly interesting for two groups of people: Smart Toys manufacturers (to decide which features and elements include in their devices) and final users (to take informed decisions).

Future lines of work

Along the development of this project and as a conclusion for it, there have been identified possible and interesting future lines of work which are presented next:

(i) The possibility of complete and bring to a low-level of detail the presented development, with the purpose of providing a higher level of accuracy while identifying risks and mitigations.

(ii) To develop a commercial solution based on the proposed methodology, such as the mentioned gateway, that would allow users to easily identify the security risks that they are exposing themselves to in an IoT environment. Such a resource would not only help to prevent or mitigate active risks for children and their families, but also to spread a security information culture among the most vulnerable agents (users). Moreover, this solution could also be presented as a business solution that would allow providers of Smart Toys to identify and correct their risk sources before deploying their solutions, preventing them from great money losses as a consequence of fines or reputation damages, among others.

REFERENCES

[1] Gartner, "Leading The IoT," 2017. [Online]. Available: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf. [Accessed 26 February 2019]

[2] Mozilla, "Internet Health Report 2018," 10 April 2018. [Online]. Available: https://internethealthreport.org/2018/introduction/how-healthy-is-the-internet/. [Accessed 26 February 2019]

[3] ESET, "5 ways to protect your internet of things," 3 April 2017. [Online]. Available: https://www.eset.com/us/about/newsroom/corporate-blog/survey-internet-of-stranger-things/. [Accessed 29 February 2019].

[4] "New rules to prevent children's 'smart' toys from being hacked," 21 November 2018. [Online]. Available: https://www.itv.com/news/2018-11-21/new-rules-on-internet-toy-security/. [Accessed 26 February 2019].

[5] R. Minerva, A. Biru and D. Rotondi, "Towards a definition of the Internet of Things (IoT)," IEEE, 27 May 2015. [Online]. Available: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf. [Accessed 26 February 2019].

[6] ENISA, "Baseline Security Recommendations for IoT," 20 November 2017. [Online]. Available: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

[7] P. DeBeasi, "Architect IoT Using the Gartner Reference Model," 26 April 2018. [Online]. [Accessed June 2018].

[8] M. Burhan, R. Asif Rehman, B. Khan and B. S. Kim, "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey," PMC, 24 August 2018. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC61654 53/. [Accessed 26 February 2019].

[9] Federal Trade Commission, "Children's Online Privacy Protection Rule ("COPPA")," [Online]. Available: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule. [Accessed 26 February 2019].

[10] Regulation GDPR," European Parliament and the Council, 27 April 2016. [Online]. Available: https://gdpr-info.eu/. [Accessed 26 February 2019].

[11] INCIBE, "INCIBE y la Asociación Española de Fabricantes de Juguetes publican una guía para el uso seguro de los juguetes conectados," INCIBE, 11 December 2018. [Online]. Available: https://www.incibe.es/sala-prensa/notas-prensa/incibe-y-asociacion-espanola-fabricantes-juguetes-publican-guia-el-uso. [Accessed 26 February 2019].

[12] OWASP, "IoT Attack Surface Areas," 29 November 2015. [Online]. Available: https://www.owasp.org/index.php/IoT_Attack_Surface_Areas. [Accessed 26 February 2019].

[13] NISTIR, "Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)," February 2018. [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/8200/draft

[14] R. Shahan and B. Lamos, "Internet of Things (IoT) security architecture," Microsoft Azure, 10 September 2018. [Online]. Available: https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture. [Accessed 26 February 2019].

[15] Motherboard, "One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids," 27 November 2015. [Online]. Available: https://motherboard.vice.com/en_us/article/yp3z5v/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids. [Accessed 26 February

[16] T. Hunt, "Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages," 28 February 2017. [Online]. Available: https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/.

[17] P. Stone, "Hacking Unicorns with Web Bluetooth," 28 February 2017. [Online]. Available: https://www.contextis.com/blog/hacking-unicorns-web-bluetooth.

[18] Change.org, "Drop the "Hello Barbie" Eavesdropping Doll," 2015. [Online]. Available: https://www.change.org/p/mattel-drop-the-hello-barbie-eavesdropping-doll. [Accessed 26 February 2019].

[19] C. Baraniuk, "Call for privacy probes over Cayla doll and i Que toys," 6 December 2016. [Online]. Available: https://www.bbc.com/news/technology 38222472. [Accessed 26 February 2019]

[20] A. Liptak, "Amazon's Alexa started ordering people dollhouses after hearing its name on TV," 7 January 2017. [Online]. Available: https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse. [Accessed 26 February 2019].

Paula González Domínguez (paulagonzalezdom@gmail.com) is a Senior Consultant at Deloitte. She received a MSc in Cyber Security by the UNIR (Universidad Internacional de La Rioja) in 2018, with honors in her Master's Thesis. Her work and research are focused on Infrastructure Protection, Security Risk Assessment, Cybersecurity Strategy and Awareness.

Fidel Paniagua Diez (fidel.paniagua@uc3m.es) is a researcher in the Evalues Lab (IT Security Evaluation) at Carlos III University of Madrid and is pursuing a PhD in computer security. His research interests include access control models and designing, developing, and evaluating secure communication systems. Paniagua Diez's PhD work is part of the research project SAVIER (Situational Awareness Virtual Environment), supported by Airbus Defense and Space. He received a BSc in computer engineering from Carlos III University of Madrid. He is Certified Ethical Hacker and EC-Council Certified Security Analyst.

Diego Suárez Touceda (diego.suarez@unir.net) is Associate Professor and Researcher at UNIR (Universidad Internacional de La Rioja) and Key Account Manager and Sr. Cybersecurity Expert at Clover Technologies S.L. He is Ph.D. in Information Security, CISM, CISSP, CEH and ECSA. His work and research are focused on Security Architectures, Network Security Services, Access Control Systems, Cybersecurity, Wearable Devices, P2P Systems, IoT, Smart Cities and Cloud Computing.

Juan José Nombela Pérez (juanjose.nombela@unir.net) is academic director of the master's degree on Cyber Security at UNIR (Universidad Internacional de La Rioja). He received a MSc in Cyber Security from Polytechnic University of Madrid and he is CISA, CISM and 27001 Lead Auditor. His work and research are focused on Biometric Security, Network Security, Mobile Device Security, Identity Management and Security management.