Identifying Long-Term Risks of the Internet of Things

Erik Buchmann

Hochschule für Telekommunikation Leipzig,
Gustav-Freytag-Str. 43-45, 04277 Leipzig, Germany
Email: buchmann@hft-leipzig.de

Andreas Hartmann

Hochschule für Telekommunikation Leipzig,
Gustav-Freytag-Str. 43-45, 04277 Leipzig, Germany
Email: hartmann@hft-leipzig.de

***Abstract*—The Internet of Things is a result of decades of research in Ubiquitous Computing and Mobile Computing. It comes with many advantages for businesses, industry and consumers. Typical examples are a seamless integration of physical objects into digital workflows and improved modes of use for consumer products. However, if non-smart devices are replaced by smart ones, the integrated IT components might generate new risks that stem from different lifecycles of embedded software, libraries and protocols used, and the IT ecosystem needed. We strive for an exhaustive catalog of long-term risks for the operational life-span of smart devices. To this end, we describe an approach to identify risks which might materialize years after a smart device has been rolled out and purchased. Furthermore, we present the risks for a fragment of a smart device's ecosystem we have identified so far.**

***Index Terms*—Internet of Things; Security; Risk Management**

I. INTRODUCTION

In the last years, advances in hard- and software in the area of Ubiquitous Computing and Mobile Computing have led to numerous industrial components and consumer products that have been equipped with sensors, computational resources and communication interfaces, e.g., to cloud services. Together, such smart devices form the Internet of Things (IoT) [1]. In many cases, smart devices stem from non-smart predecessors. For example, a modern smart TV looks and feels mainly like a classical non-smart one with some extras.

Using smart devices comes with a plethora of benefits. From a business perspective, IoT technology promises to reduce process costs, increase process speeds, allow for in-depth process monitoring or new options to integrate logistics processes or manufacturing processes with business activities. For consumers, IoT allows to create smart homes with devices that can be controlled remotely via smartphone, adapt to the user's habits, and provide convenient services locally or over the Internet. However, public and specialized media provides anecdotal evidence that smart devices might come with operational risks that appear after roll-out. With a familiar non-smart device in mind, the customers might not expect such risks when deciding for a smart device.

Example 1: Software and hardware lifecycles are different. *The device's software lifecycle might be much shorter than the hardware's operational capability. Consider a smart TV based on the Android TV operating system. Its software receives security updates for about three years. Thus, after three years the smart TV becomes a security issue [2], even if the hardware is still in good condition and fully operational.*

Example 2: Loss of control. *Smart devices may depend on a cloud service. For example, after a third-party service provider stopped its business, tens of thousands smart Internet radios became non-functional [3] without warning in advance.*

Example 3: Changing compliance or legislation. *Changes in the legislation may restrict the use of smart devices after years of operation. Consider a smart security camera generates burglar alerts via cloud service in the UK. Under the ongoing discussion of the Brexit [4] and the EU General Data Protection Regulation [5] (GDPR), it remains unclear under which conditions person-related videos can be sent to a cloud in the UK.*

In order to make smart devices accessible for risk management approaches, a comprehensive catalog of potential risks is required. However, to the best of our knowledge, existing approaches don't focus on long-term operations and have a narrow topic, e.g., IT security. We are interested in risks that materialize years after a smart device has been purchased. Thus, we define our problem statement as follows:

Which specific risks for the continued long-term use of smart devices may materialize after purchase, but cannot be expected from a smart device's non-smart predecessor?

We call an appliance a "smart device", if it contains computational capabilities and data links, which were not needed for the primary function of its non-smart predecessor. For example, a classical TV did not need Internet access to display live TV programmes. With "long-term" we refer to the operational time that can be expected from the device's hardware. Intuitively, this is the expectation of a naive customer who replaces a broken non-smart device with a new smart one.

In this paper, (1) we propose a research approach to systematically derive such risks, and (2) we exemplary outline the risks we have identified for one fragment of a smart device's infrastructure.

Paper outline: In Section II, we briefly discuss related work. In Section III, we sketch our approach to identify long-term IoT risks. In Section IV, we describe risks we have identified. Section V concludes.

ISBN: 978-1-61208-811-2

II. Related Work

a) Risk Analyses for IoT: Advances in technology call for risk analysis before adoption. However, all risk analysis approaches we are aware of focus on the current situation and have a narrow perspective, e.g., on current IT security or return of investment. For example, [6] provides an exhaustive view on the vulnerabilities of smart devices in the consumer market. The risk assessment approach described in [7] considers the management of risk in the past two years, but does not feature a projection in the future, e.g., when security breaches for a discontinued product remain untreated. In consequence, existing approaches that deal with IoT risks over the product lifetime [8], [9] don't consider that vendors may loose interest in supporting discontinued products, or that it will be hard to find experts to maintain outdated technology.

b) Design Science Research: Design science research [10] is a method where an artefact is constructed from a knowledge base, evaluated and improved in multiple rounds. Those rounds can be structured in three cycles of activities. The *relevance cycle* specifies and refines the use cases needed to construct the artefact and to evaluate its applicability. The *rigor cycle* builds a knowledge base from literature and experience that is needed to evaluate the novelty and research contribution of the artefact. The central *design cycle* iterates between building and evaluating the artefact, based on information from the other cycles.

c) BSI-Standard 200-3: The BSI-Standard 200-3 [11] for risk analysis based on IT-Grundschutz defines a process that allows organizations to assess their information security risks. For this purpose, the standard defines the steps necessary for risk identification, risk assessment and risk treatment. In this paper we focus on risk identification. The standard separates (a) non-specific, elementary threats, as fire, theft, misconfiguration or manipulation, and (b) specific threats arising from specific scenarios. Furthermore, the standard provides the means for risk classification and consolidation.

d) Long-Term Digital Preservation: A problem that has been extensively discussed in the past years is the preservation of digital contents over time [12]. The risks for digital content [13] overlap with the risks of using an out-of-date smart device in a modern environment. Examples are media obsolescence and format obsolescence [13], i.e., the digital object cannot be read with current devices due new media or new formats. Security properties have been established with protocols that are insecure now [14]. Digital objects such as dynamic web pages [15] or computer games [16] require a complex execution environment.

III. How to identify Long-Term IoT risks

In this section, we describe our research method. To systematically identify long-term risks for the use of smart devices, we have adapted BSI-Standard 200-3 [11] so that it creates the knowledge base and designs a risk catalog that fits into relevance and design cycle of Design Science Research [10]. We use research literature to foster the rigor cycle. In particular, we define the following steps:

1) Determine a number of relevant use cases. On this basis, model a generic IT infrastructure that fulfils the requirements for a smart device and its non-smart counterpart to operate as intended.
2) Analyse each artefact in the infrastructure for the smart device in isolation. Determine under which conditions this artefact operates as intended at time of purchase.
3) Consider this condition a potential risk, if the condition doesn't exist at time of purchase and doesn't materialize in the non-smart device's infrastructure.
4) Consolidate risks that are identical for multiple artefacts. Categorize similar risks and remove elementary ones.
5) Back up each individual risk by literature in order to evaluate the plausibility of the risks identified.
6) Repeat these steps with different use cases until no further risks are identified.

For illustration, we apply this approach to Example 3 from the introduction. *Step 1:* The generic IT infrastructure for the smart security camera contains, among other things, a data connection between the smart device and a cloud service provider in the UK. This is because the security camera vendor has outsourced the burglar alert into the cloud. The connection transports personal data, e.g., videos of humans. *Step 2:* One required condition is that the data transfer is legal - depending on the legislation. *Step 3:* A common non-smart security camera uses a local storage system, not needing a legal authorisation for cross-border data transfers. *Step 4:* "Changing privacy legislation for data transfers into other countries" is not an elementary risk. *Step 5:* A body of literature can be identified, discussing the risks of changes in the privacy regulations for transferring data to a UK cloud, e.g., [4]. Thus, we have identified "changing privacy legislation" as a plausible risk for *any* smart device that uses such an IT infrastructure to transfer personal data.

IV. Categories of long-term risks

In this section, we describe the outcomes of our ongoing research according to the six steps defined in Section III.

a) Use Cases and IT Infrastructure Model: According to Step 1 of our research method, we started our analysis by determining a set of relevant use cases. To this end, we have selected three smart devices that have different purposes:

- A **smart TV** (Philips Ambilight 32PFS6402),
- a **smart security camera** (Reolink RLC-410) and
- a **smart speaker** (Amazon Echo) with voice assistant.

Following our method, we created a generic IT infrastructure model from those use cases. Our model considers data, organizations, processes, devices and connections.

ISBN: 978-1-61208-811-2

TABLE I. Categories of data.

Id	*Name*	*Description*
D1	Sensor Data	Raw sensor information, such as unprocessed video and audio feeds, GPS and WLAN localization data or keystrokes from a remote control.
D2	Operational Data	Data needed to execute the device's function, e.g., commands to activate the smart speaker or a live video stream from the camera.
D3	Meta-Data	Time stamps, transmission information, character encoding, session keys etc. from the algorithms and protocols used.
D4	Configuration	Data that defines the behavior of the device, including updates, private keys and certificates.
D5	Telemetry	Data used to supervise the behavior and use of the device.

Table I contains the categories of data of our infrastructure model. We consider D1 - D5 as personal data according Art. 4 No. 1 GDPR [5]. A time series of D1, D2, D3 or D5 allows to construct a fingerprint of the device and/or of the user's activities. D4 contains unique logins for cloud services and personal settings. Thus, a relation to a single person can be determined, even there are no personally identifiable information generated, such as user name or image.

TABLE II. Categories of organizations.

Id	*Name*	*Description*
O1	User	The user of the smart device.
O2	Vendor	The vendor of the device.
O3	Cloud	The provider and operator of the cloud service.
O4	External	Any third party.

Table II describes the categories of organizations our model considers. Service operation may vary between O2 (Infrastructure as a Service) or O3 (Software as a Service). With O4 we refer to any external party that is invoked from the smart device. For example, Amazon's smart speaker can access the Google calendar or a Philips smart light bulb.

TABLE III. Categories of processes, assigned with data.

Id	*Name*	*Data*	*Description*
P1	Updates	D2, D3, D4, D5	All functional updates and security updates.
P2	Local Ops	D1, D2, D3, D4	Any operation that is processed locally on the device.
P3	Cloud Ops	D1, D2, D3, D4, D5	Any operation that is processed remotely in the cloud.
P4	External Ops	D1, D2, D3	Any operation that is processed by a third party.
P5	Telemetry	D3, D4, D5	The vendor supervising the behavior of the smart device.

The categories of processes are listed in Table III, together with the categories of data used. A process activity can be initiated by a local operation (P2), handed over for analysis to the cloud service (P3) and is executed as an external operation (P4). For example, an Amazon Echo recognizes the activation code "Hi Alexa" locally and sends an audio feed containing the sentence "Turn on all lights." to the Amazon cloud. The Amazon cloud service performs natural language processing, recognizes the commands and sends them to a Philips cloud service. Then, the Philips service activates the local light bulbs.

TABLE IV. Categories of devices, assigned with organizations.

Id	*Name*	*Organization*	*Description*
G1	Device	O1	The smart device itself.
G2	Cloud	O2, O3	The cloud service.
G3	ext. Device	O1, O3, O4	Any external device.

Table IV contains the categories devices and the organizations operating them. We have left aside the router needed to connect the smart device to the Internet. Our risk identification process has shown that any risk involving the router is an unspecific elementary risk. With "external Device" we refer to any situation where a third device is involved. This might be the user's smartphone, a virtual gadget in the cloud that is operated by a third party, or a smart home installation that is under control of the smart device.

TABLE V. Categories of connections, assigned with data.

Id	*Devices*	*Data*	*Description*
C1	G1 – G2	D1, D2, D3, D4, D5	Bidirectional connection: smart device– cloud.
C2	G2 – G3	D1, D2, D3	Bidirectional connection: cloud – external device.

Finally, Table V enumerates the categories of connections between the devices and the data transferred with each connection. If earphones, external storage, etc. is connected to the smart device, the associated risks are identical for smart and non-smart devices. Our use cases don't allow a direct connection between the smart device and an external device beyond that. For the time being, we assume any data transfer to an external recipient is managed by a cloud service.

b) Long-term risks for C2: Steps 2 to 5 of our research method let us identify and consolidate the long-term risks for each component of our infrastructure model. Furthermore, we have to filter risks that are specific for smart devices, and we need to substantiate them with literature. For the sake of brevity, we exemplary describe only the risks we have identified for the connection between the cloud service and an external device (Artefact C2). For each risk, we present only one example from literature to confirm it's existence.

After having consolidated the risks according to Step 4, we have learned that C2 has risks in three different areas. Table VI shows the compliance risks we have identified, Table VII contains the economic risks, and Table VIII lists the operational risks.

TABLE VI. Long-term compliance risks associated with C2.

Risk	*Description*
Legislation	Changing legislation, new codes of conduct, new trade restrictions etc. impose limitations on the exchange of personal data with certain countries or parties [4].
Expiration	Disagreements to common compliance standards, expired certifications or approvals, non-renewed audits, etc., render the connection untrusted [17].
Concealment	Characteristics that were hidden at roll-out ban the connection by law, e.g., if it becomes known that personal information is sent to external parties without the customers consent [18].

TABLE VII. Long-term economic risks associated with C2.

Risk	*Description*
Degradation	For economic reasons the service quality of the connection will be reduced, e.g., by applying bandwidth throttling in favor of other services [19].
Licensing	The revenue model might change. For example, the external party might switch to a pay-per-use model which makes external connections expensive [20].
Discontinuation	One of the parties involved discontinues its service or makes it uneconomic. Patents, licenses etc. disallow to continue the service with other parties [21].
Liabilities	One of the parties involved discontinues its business, and its contractual liabilities become void [22].

TABLE VIII. Long-term operational risks associated with C2.

Risk	*Description*
Inflexibility	Without updates for new formats, protocols or interfaces, it becomes challenging to connect to more recent services or devices, or to adapt to new modes of service [23].
Unreliability	The service level in terms of reliability, throughput, etc. of the connection degrades, e.g., due to reduced support for end-of-lifetime products [24].
Unmaintainability	Due to the use of outdated formats, protocols or interfaces and closed-source components it becomes difficult to find experts or spare parts needed to that maintain the connection [25].
Insecurity	Without security updates and by using out-of-date security protocols, the connection does not meet the required level of security any more [24].
Defectiveness	Modernizations in the IT ecosystem make technical debts visible, e.g., if header fields reserved for future use in transmission protocols were not handled according to the standard [26].

Recall that the tables contain the long-term risks for C2. An example for a risk for other fragments (G1–G3) is the absence of experts for today's high-tech components, that are outdated in the future. Every year, employees with expert knowledge retire, but new starters do not learn to use out-of-date technology. Considering the innovation cycles, this will become an issue when operating smart devices in the future.

As part of our ongoing research, we will follow the steps listed in Section III. We strive to identify a comprehensive set of long-term risks for all infrastructure artefacts from all categories. For this purpose, we will identify and consolidate such risks for all artefacts of our infrastructure model, and we will extend the model by further smart devices.

V. Conclusion

The Internet of Things is a promising approach from the area of Ubiquitous Computing and Mobile Computing to integrate physical objects into computing environments. However, if non-smart devices are replaced by smart IoT devices, the integrated IT components might generate new risks that stem from different lifecycles of digital and physical objects, and the IT ecosystem needed.

In this paper, we have developed an approach to identify risks which might materialize years after the purchase of a smart device. Furthermore, we described the risks we have identified for a fragment of a smart device's ecosystem. It is part of our future work to compile an exhaustive catalog of long-term risks for the operational life-span of smart devices.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] B. Schoon, "Android tv needs better standards for long-term updates and support," https://9to5google.com/2019/08/29/android-tv-long-term-updates-support/, 2019, retrieved: 2020-06-09.

[3] Frontier Nuvola Support, "Why did the service change on the 7th may 2019?" https://srsupport.frontier-nuvola.net/portal/kb/articles/service-change, 2019, retrieved: 2020-06-10.

[4] K. McCullagh, "Brexit: potential trade and data implications for digital and fintech industries," *International Data Privacy Law*, vol. 7, no. 1, p. 3, 2017.

[5] Council of the European Union, "Regulation (eu) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data," OJ L 119, 4.5.2016, p. 1–88, 2016.

[6] T. Alladi, V. Chamola, B. Sikdar, and K.-K. R. Choo, "Consumer iot: Security vulnerability case studies and solutions," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17–25, 2020.

[7] M. Aydos, Y. Vural, and A. Tekerek, "Assessing risks and threats with layered approach to internet of things security," *Measurement and Control*, vol. 52, no. 5-6, pp. 338–353, 2019.

[8] O. Garcia-Morchon *et al.*, "A comprehensive and lightweight security architecture to secure the iot throughout the lifecycle of a device based on himmo," in *Symposium on Algorithms and Experiments for Wireless Sensor Networks*, 2015.

[9] J. L. Hernández-Ramos, J. B. Bernabé, and A. Skarmeta, "Army: architecture for a secure and privacy-aware lifecycle of smart objects in the internet of my things," *IEEE Communications Magazine*, vol. 54, no. 9, pp. 28–35, 2016.

[10] A. Hevner and S. Chatterjee, "Design science research in information systems," in *Design research in information systems*. Springer, 2010, pp. 9–22.

[11] Bundesamt für Sicherheit in der Informationstechnik, "BSI Standard 200-3: Risk Analysis based on IT Grundschutz," *https://www.bsi.bund.de*, 2017, retrieved: 2020-08-08.

[12] Digital Preservation Coalition, "Digital preservation handbook," https://www.dpconline.org/handbook, 2015, retrieved: 2020-06-09.

[13] S. Vermaaten, B. Lavoie, and P. Caplan, "Identifying threats to successful digital preservation: the spot model for risk assessment," *D-lib Magazine*, vol. 18, no. 9/10, pp. 1–21, 2012.

[14] H. M. Gladney, "Trustworthy 100-year digital objects: Evidence after every witness is dead," *ACM Transactions on Information Systems (TOIS)*, vol. 22, no. 3, pp. 406–436, 2004.

[15] G. TRUMAN, "Web archiving environmental scan: Harvard library report," *Digital Access to Scholarship at Harvard*, 2016.

[16] J. Andersen, "Where games go to sleep: the game preservation crisis," https://www.gamasutra.com/view/feature/134653/where_games_go_to_sleep_the_game_.php, 2011, retrieved: 2020-06-09.

[17] Y. T. Mak, S. Carr, and J. Needham, "Differences in strategy, quality management practices and performance reporting systems between iso accredited and non-iso accredited companies," *Management Accounting Research*, vol. 8, no. 4, 1996.

[18] J. C. Roberts and W. Al-Hamdani, "Who can you trust in the cloud? a review of security issues within cloud computing," in *Information Security Curriculum Development Conference*, 2011, pp. 15–19.

[19] D. A. Lyons, "Net neutrality and nondiscrimination norms in telecommunications," *Arizona Law Review*, vol. 54, p. 1029, 2013.

[20] M. A. Cusumano, "The changing software business: Moving from products to services," *Computer*, vol. 41, no. 1, pp. 20–27, 2008.

[21] M. A. Lemley and T. Simcoe, "How essential are standard-essential patents," *Cornell Law Review*, vol. 104, p. 607, 2018.

[22] A. Schwartz, "Products liability, corporate structure, and bankruptcy: toxic substances and the remote risk relationship," *Journal of Legal Studies*, vol. 14, no. 3, pp. 689–736, 1985.

[23] P. Mutchler *et al.*, "Target fragmentation in android apps," in *IEEE Security and Privacy Workshops*. IEEE, 2016, pp. 204–213.

[24] B. Ford, "Icebergs in the clouds: the other risks of cloud computing," in *4th USENIX conference on Hot Topics in Cloud Computing*, 2012.

[25] L. M. D. Ferreira, A. Arantes, and C. Silva, "Discontinued products," in *Conference on Operations Research and Enterprise Systems*, 2017.

[26] P. Kruchten, R. L. Nord, and I. Ozkaya, "Technical debt: From metaphor to theory and practice," *IEEE Software*, vol. 29, no. 6, pp. 18–21, 2012.