Privacy risk analysis in the IoT domain

Juan Hernández-Serrano, Jose L. Muñoz, Olga León
Universitat Politcnica de Catalunya
Barcelona, Spain

Lars Mikkelsen, Hans-Peter Schwefel
Aalborg Universitet
Aalborg, Denmark

Arne Bröring
Siemens AG
Munich, Germany

***Abstract*—Most IoT systems are using or exchanging user related information between system components. This means that privacy is a key factor in these systems. Privacy, both in terms of not allowing unauthorized access to information, but also in terms of handling sensitive information correctly and responsibly. As IoT systems typically are comprised of many software and hardware distributed components, ensuring privacy is a challenging task. This paper proposes a risk rating methodology for identifying and rating privacy risks, and demonstrates how to apply this methodology in an IoT use case set in the context of the EU H2020 BIG IoT project. It is also demonstrated how to handle the results of the risk rating methodology.**

***Index Terms*—Risk assessment; Internet of Things; IoT; security; privacy;**

I. Introduction

In the past years, the Internet of Things (IoT) has largely expanded and the number of IoT devices is evermore increasing. Today, IoT use cases span over a wide variety of application domains, ranging from smart homes over e-health systems to industrial environments. Things used in such applications are made available through IoT platforms. These platforms can be located on the device, fog, or cloud level.

A multitude of such platforms exist today. In order to enable cross-platform and even cross-domain application development, different initiatives are determined to form IoT ecosystems. An example for such an ecosystem initiative is the European H2020 BIG IoT project[1] [1].

BIG IoT has two main objectives. The first one is defining a shared interface, i.e., the so-called BIG IoT API comprising common functionalities such as service discovery, access, and event handling. This API needs to be supported by all participating platforms, often in addition to their existing proprietary interface, as illustrated in figure 1. The second objective is establishing a centralized marketplace where platforms as well as value-adding services can be registered, searched, and subscribed by applications. In the BIG IoT project, these technologies are deployed in multiple pilot scenarios and involving various IoT platforms, services, and applications from the Smart Cities domain.

Besides the evident benefits that can be achieved by such IoT ecosystems, dealing with security and privacy in the IoT is more challenging and more complex than it is in conventional networks, mainly by 4 reasons: 1) a very dynamic set of services and applications intensively handling data types with also very dynamic formats; 2) a multitude of usage scenarios,

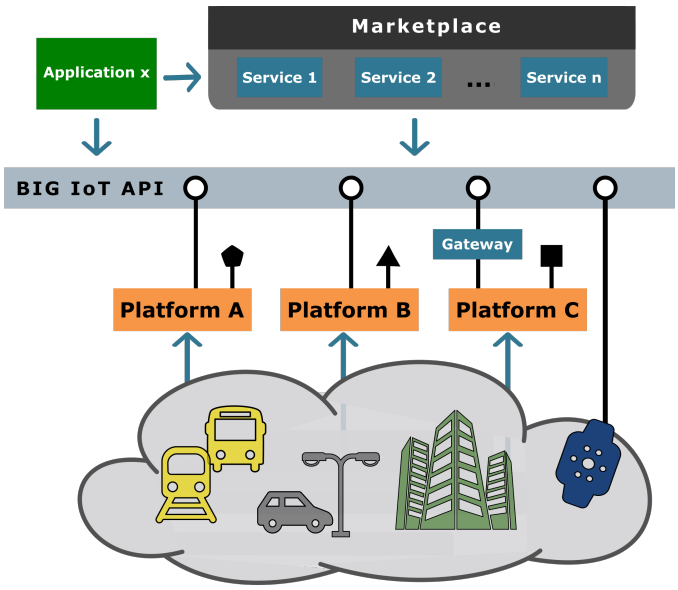

Figure 1. The BIG IoT approach for building an ecosystem of IoT platforms (source: [2]).[2]

stakeholder settings for data provisioning and usage; 3) the high speed of information propagation and tool development in an IoT ecosystem; and 4) the lack of a simple security methodology that does not rely on long lists of factors that are complex to apply.

The continued growth of IoT ecosystems will heavily depend on properly addressing the security and privacy challenges that come from them.

Among the different security and privacy requirements that have been identified to ignite a secure and reliable IoT ecosystem [2], **privacy by design** is key. Indeed, it has been literally requested ("Data protection by design" - DPD) in the Article 25 of the General Data Protection Regulation [3], which will become enforceable from May 2018.

DPD refers to building privacy features from the very beginning of the design process instead of modifying or adding new features at a later stage. This fact involves the consideration of privacy in the full software development life cycle (SDLC). Notice that introducing privacy in the SDLC does not necessarily imply added costs. The cost of a data breach differs for every organization. As stated in [4], on average, all organizations in European countries such as France

[1]http://big-iot.eu

[2]Icons by Freepik from http://www.flaticon.com

and Germany will incur the cost of at least 3 million euros for a data breach. According to this, investing in DPD should be understood as a factor of economical savings and not the other way round. It can help in saving direct operational costs due to data breaches and indirect cost due to the consequent loss of reputation.

However, the appropriate privacy measures will strongly depend on the identified risks. In the end, security always comes down to making a risk assessment. Identifying the risks is of paramount importance in order to fully understand the security and privacy threats and to support a mitigation strategy. A risk rating methodology (RRM) is therefore key to establish metrics that allow to evaluate the severity of the vulnerabilities. Therefore, every identified issue should have a corresponding score that should allow to properly prioritize how and when it is addressed on the SDLC. An appropriate RRM can also be a valuable tool to achieve compliance with the GDPR in a near future.

There are several proposals for risk analysis in specific IoT ecosystem [5]–[7] as well as many works identifying privacy issues, challenges and implications [8]–[10]. However, to the best of our knowledge, there is not yet a clear methodology for the analysis and integration of privacy-related risk assessment results into the SDLC, in a sense of properly assigning a priority to development issues/actions derived from the analysis.

The rest of the paper is organized as follows. In section II we present an adaptation of the Open Web Application Security Project (OWASP) RRM, defined in [11], to the specifics of an IoT ecosystem, in particular the BIG IoT ecosystem. The target is to provide a simple but effective methodology that could easily mark the identified risks and include them into the SDLC as software issues to be addressed with an appropriate priority. The proposed methodology is specifically tuned to analyse online IoT platforms and services with regard to privacy risks. Moreover, it is also shown how the results of the risk assessment are transformed into development issues that are addressed in the SDLC. A use case example in the BIG IoT project is presented in section III. Finally, conclusions are drawn in section IV.

II. From the OWASP risk rating methodology to a BIG IoT risk rating methodology

Integrating security and privacy analysis into the SDLC will lead to costs saving by early discovery and fixing of vulnerabilities. There are many approaches to risk analysis [12]–[14], where the OWASP-proposed methodology [12] is considered in this work.

The OWASP RRM is a general-purpose RRM that covers evaluation of the potential attacker, the exploit evaluation and detection, and finally, the evaluation of the technical and business impact in different domains. In our scenario, the domain is limited to IoT, and specifically to exchange of data and services related to IoT. Specific for the IoT domain is that IoT platform collect and process big quantities of data from myriads of sensor units. The collected data is then used by services and applications to provide services to users, sometimes also based on input from users.

A. Risk evaluation

We focus on the risk analysis of privacy and data breaches and their consequences in the IoT scenario. With such a purpose, we consider as baseline the risk factors of the OWASP RRM. Then, we select and tune the factors that are relevant for our scenario and we also propose new key factors that, from our point of view, are lacking in OWASP RRM.

Once we have the list of factors, as detailed below, we score the factors from 1 to 9, where 1 is low impact or likelihood and 9 is high. Unlike with the OWASP approach, we also assign weights to the factors considering the idiosyncrasy of the analysed scenario.

The overall likelihood and impact (both technical and business) are computed as the weighted arithmetic mean of their factors. Therefore, the overall values are calculated by taking the sum of the scores multiplied by their weights and dividing by the sum of the weights. Estimating the associated risk to the business is just as important, since the resources available to fix the vulnerabilities will often depend on it.

The results are then classified into 3 levels; 0 to 3, 3 to 6, and 6 to 9, which are denoted as **`low`**, **`medium`** and **`high`** respectively. Finally, the risks are evaluated by combining impact and likelihood by using table I. Additionally, we have two interesting edge cases which will have particular names:

- **`critical`**: these are risks with high probability and high impact attacks. These risks are the ones that should be addressed by the company in first place.
- **`negligible`**: these are risks with low probability and low impact attacks. A company may not address them or just ignore them depending on the available resources.

Table I
Overall risk severity indication based on the detected impact and likelihood

	Likelihood		
Impact	`low`	`medium`	`high`
`high`	**`medium`**	**`high`**	**`critical`**
`medium`	**`low`**	**`medium`**	**`high`**
`low`	**`negligible`**	**`low`**	**`medium`**

Following, we show the selected factors for the risk analysis and their weights.

B. Weighting of factors

In the following, we explain the factors, we estimate how they should be computed, and how they are weighted. The weights depend on how relevant the various factors are in the IoT scenario, and which factors are more important than

others. As a starting point all factors are assigned the weight of 1 and then reduced according to importance and relevance, and factors with 0 weight are dropped.

1) Threat agent factors:

a) Skill level: Weight: 1. This factor describes the required skill level of the attacker to perform the attack, which is relevant in determining how realistic the exploit is. Note the description is changed from the OWASP description. Security penetration skills (1); advanced computer user (5); no technical skills (9).

b) Motive: Weight: 0.5. This factor describes how motivated the attacker is to perform the exploit. The importance of this factor in BIG IoT is currently reduced, since the focus of the risk analysis is to evaluate the severity of data breach, and to a lesser extent the payoff of the attacker. Low or no reward (1); possible reward (5); high reward (9).

c) Opportunity: Weight: 1. This factor describes the opportunity or resources needed to perform the exploit. Much like the skill level, this factor also helps in determining how realistic the exploit is. Full access or expensive resources required (1); Special access or resources required (5); Can be done by readily available off-the-shelf equipment, without any constraints on physical presence or special software (9).

d) Size: Weight: 1. This factor describes the scope of the attack, i.e. in terms of how large the group of potential victims is. Note the description is changed from the OWASP description. Just one (1); tens of individuals (5); thousands (9).

2) Vulnerability factors:

a) Ease of discovery: Weight: 0.25. This factor describes how easy it is for attackers to discover the exploit. Due to the speed at which knowledge of exploits spread on the Internet, the importance of this factor is reduced, as it is less important if it is easier or harder to discover. Practically impossible (1); difficult but possible (5); automated tools available (9).

b) Ease of exploit: Weight: 0.25. This factor describes how easy it is to perform the exploit and to obtain access to functionalities or data, but also in terms of how much effort must be spent to be able to take advantage of the functionalities or data. The importance of this factor is reduced because it should be assumed that if an exploit exists, then automated solutions will appear over time for exploiting it. For this reason the factor has less impact. Theoretical (1); difficult but possible (5); automated tools available (9).

c) Awareness: Weight: 0.25. This factor describes how aware potential attackers are of this exploit. Its importance is reduced due to the speed with which exploits and tools utilizing them are propagated. This means that if only a few attackers are aware of the exploit today, this will change rapidly. Unknown (1); hidden (5); public knowledge (9).

d) Intrusion detection: Weight: 1. This factor describes the capability of detecting if the exploit is utilized, i.e. in terms of logging access. Active detection in application (1); logged and reviewed (5); not logged (9).

3) Technical impact factors:

a) Loss of privacy: Weight: 1. This factor describes how accurately the functionalities or data exposed via the exploit allow an attacker to track users or their actions. Note this is a new factor not defined in OWASP. Minimal non-sensitive data disclosed (1); Minimal critical data disclosed to extensive non-sensitive data disclosed (5); Personal information that is directly linked to an individual (9).

b) Loss of accountability: Weight: 0.5. This factor describes to what extent the actions of an attacker are traceable. Its importance is reduced because it is of less importance to be able to identify the individual attacker. Fully traceable (1); possibly traceable (5); completely anonymous (9).

4) Business impact factors:

a) Financial damage: Weight: 0.5. This factor describes the financial impact of the exploit, i.e. in terms of how much the business or business model is financially affected. The importance of this factor is reduced because the financial impact will vary for different cases, and for this reason should not be a determining factor of the risk evaluation. Furthermore, this methodology focuses on a general IoT ecosystem. Less than the cost to fix the vulnerability (1); some effect on annual profit (5); bankruptcy (9).

b) Reputation damage: Weight: 0.5. This factor describes the damage to the reputation of the business based on the exploit. The importance of this factor is reduced because influence on reputation will have different impact on different businesses, and again this methodology focuses on a general IoT ecosystem. For this reason this factor should not be a determining factor of the risk evaluation. Minimal damage (1); loss of goodwill (5); brand damage (9).

c) Privacy violation scale: Weight: 1. This factor describes the scale of devices and/or users affected in an exploit, i.e. how many entities are affected by the risk. Minimal scale (1); few hundreds (5); millions (9).

C. Integration with the SDLC

The last step in the risk evaluation process is to feed the results to the development cycle, so that risks can be mitigated during the next development iteration.

In figure 2 the steps of the SDLC and their ordering are illustrated next to the Risk Rating cycle. The risk rating will be done as a parallel process and the results will be fed to the SDLC as part of the Requirement Analysis step. In this way the design can be modified to handle the identified risks.

The risks with the highest severity level, i.e. critical and high, should be the first to be included in the development cycle, followed by the medium and low, and finally negligible. However, due to limited duration of development cycles, there might only be resources to mitigate the risks with the highest severity. Then another iteration of the risk analysis should be done, also focusing on new functionalities of the system, before feeding the risks to the development process as requirements.

III. Use Case Example: Environment monitoring service

We present in the following a short, simple but representative example of how the BIG IoT RRM in section II has

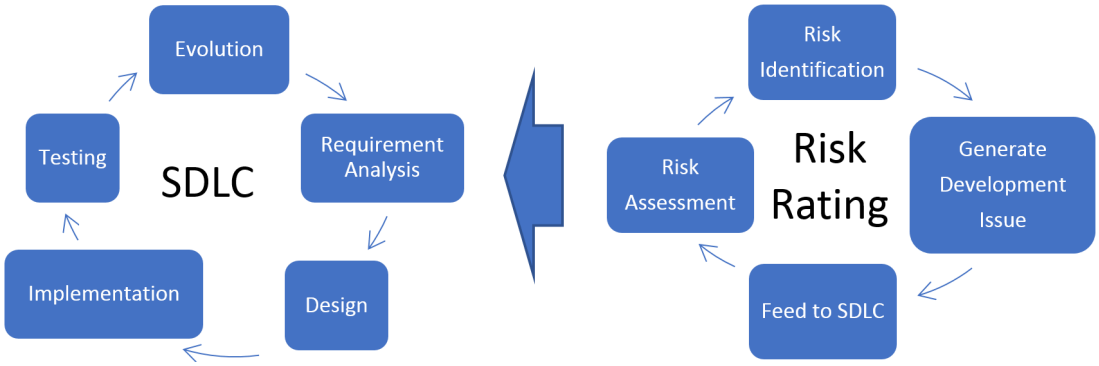

Figure 2. Illustration of how the Risk Rating works parallel to SDLC, feeding development issues into SDLC.

been applied to a BIG IoT service. The chosen BIG IoT service is the Environment Monitoring Service (EMS), which provides in a centralized manner data gathered from different environment-related offerings[3]. Currently two types of data sources are being used: pollution sensors in selected private cars and noise metering stations at different city spots.

Selected private cars. BOSCH's members in BIG IoT have installed Bezirk[4] devices in several cars provided by SEAT to the project. Installed devices can query the internal pollution sensors and offer the readings as well as the current position of the car.

Noise metering stations. Cities commonly have a deployment of noise stations that report current level of noise in specific spots. Noise data is used in the BIG IoT to compute green routes and drive vehicles through the less-noisy paths, allowing to distribute the noise and keep it under a certain threshold all over the city.

The BIG IoT security team carried out an analysis of the potential risks associated to the EMS use case. The result of the analysis identified three risks:

Vehicle/people tracking. For cars are sharing their position, an attacker could track vehicles if the shared data is not properly anonymised. Even with no identifiers, an attacker could track a vehicle computing viable trajectories based on the pairs position-time. Moreover, if a vehicle is linked to a person (e.g. by visual contact), people can be actually tracked.

Accessing/Hacking the in-vehicle internal bus. Since the Bezirk "thing" is connected to the in-vehicle information bus, if an attacker gains access to the Bezirk device, it could also try to hack the internal bus and thus eavesdrop internal/not public vehicle data and even disrupt the vehicle operation by mangling those data.

Noise level disruption. If the attacker can tamper noise data, he can influence route recommendations since the noise is a factor in these recommendations. For example, the attacker can report that an area has no noise at all. Then, many vehicles would be routed through this area (and effectively, the attacker is creating a noisy area). On the other hand, if the attacker is able to report a high level of noise, certain areas would be less considered as a routing options in route recommendations.

To keep the overall paper length short, in the following we present the application of the BIG IoT RRM for just the first risk; although, the application it is very similar for the other two ones. First, we score every factor based on the description provided in section II. Then, we derive some actions that can avoid or mitigate the identified risk. The score for the risk will be used to prioritize actions derived. Finally, we comment how the actions become issues for the SDLC and, if applied, how the risk assessment is updated.

A. *Vehicle/people tracking: Scoring*

OVERALL LIKELIHOOD: 7.95 (HIGH)

- **Skill level**. With some technical skills, an attacker should be able to track vehicles based on the identifiers provided by the EMS.
  Weight: 1 Score: 7
- **Motive**. Tracking could allow spying on specific people. Depending on the target, the motivation could be high (potential reward).
  Weight: .5 Score: 5
- **Opportunity**. The attack could be operated from any standard computer connected to the EMS.
  Weight: 1 Score: 9
- **Size**. The attack could affect thousands to millions of people.
  Weight: 1 Score: 9
- **Ease of discovery**. It should be easy to detect by basic input/output verification that the EMS is also providing identifiers or pseudo-identifiers along with the pollution and position data.
  Weight: 0.25 Score: 7
- **Ease of exploit**. Once the attacker has an array of positions and dates it is a matter of simple data processing to get the path of the victim.
  Weight: 0.25 Score: 8

[3]In BIG IoT a "offering" is a description of what a service is providing, how to access it and under what conditions

[4]Bezirk is s Startup from Bosch that was established to cater to agility in a highly dynamic environment.

- **Awareness**. Since the format of data provided by the service is published on the BIG IoT marketplace as an offering description, it is obvious to be aware of the presence of identifiers or pseudo-identifiers.
  Weight: 0.25 Score: 6
- **Intrusion detection**. The attack will not be logged since the attacker just consumes the same data as any other standard consumer.
  Weight: 1 Score: 9

TECHNICAL IMPACT: 6.33 (HIGH)

- **Loss of privacy**. An attacker can potentially track a person if it could be linked to a vehicle by another external source (e.g. by direct visual observation or by publicly accessible street cameras). Therefore, the attacker would be able to infer about the behavior about a person or a group of people.
  Weight: 1 Score: 7
- **Loss of accountability**. Since the EMS is an authenticated service, based on the attacker queries, the attack could be traceable.
  Weight: 0.5 Score: 5

BUSINESS IMPACT: 5.50 (MEDIUM)

- **Financial damage**. The knowledge of the vulnerability would probably encourage people to leave the service or to explicitly demand to not be accounted. Therefore, a strong effect on annual profit should be expected.
  Weight: 0.5 Score: 7
- **Reputation damage**. A loss of goodwill is expected in the short term regarding to this service. A full brand damage is not expected since most of the affected individuals won't see affected their privacy.
  Weight: 0.5 Score: 5
- **Privacy violation scale**. While thousands to millions tracking data of vehicles will be disclosed. Linking a vehicle identifier with a person requires very specific external information (e.g. visual contact). Therefore, the breach would likely affect no more than hundreds of people.
  Weight: 1 Score: 5

Based on the assigned scores and the data in Table I, the result of the application of the BIG IoT RRM to the EMS is depicted in Table II.

Table II
APPLICATION OF THE BIG IOT RRM TO THE EMS

Overall likelihood	`high (7.95)`
Technical impact	`high (6.33)`
Business impact	`medium (5.50)`
Technical risk severity	`critical`
Business risk severity	`high`

Based on the results of the analysis, priority actions should be carried out in order to avoid or at least mitigate this risk. Those actions are explained in the following subsection.

B. Vehicle/people tracking: Actions

To avoid potential tracking, data provided by the cars should be anonymised. Therefore, the use of identifiers or pseudo-identifiers is discouraged and, in any case, they shouldn't be stored by the service. In order to mitigate these risks the following actions should be carried out:

1) Instead of providing a measure at a given position (with GPS accuracy), provide pollution at a given area or street segment. In many cases, this fact will disable to track vehicles based on the pairs position-time. This action should be preferably implemented at device level; that is to say, in the devices already installed in the cars.
2) If possible, revisit device and service code to avoid sending potential identifiers or pseudo identifiers from the cars to the EMS.
3) Revisit service code to ensure that no potential identifiers or pseudo-identifiers are stored and/or provided by the EMS.
4) Check data already stored by the EMS (before implementing action 3) to filter out identifiers or pseudo-identifiers.

The four actions became issues that got into the SDLC of the EMS with priority `critical`, since in BIG IoT we have agreed to use the worst-case scenario (either technical or business risk). Therefore, they were fixed in a short term. In fact the EMS developing team already implemented the required actions in less than a working day.

The EMS is neither storing nor providing any identifiers. Moreover, position data has been generalized to street segments. Now, while still being useful for the purpose of green routing advice, the likelihood of linking vehicles to viable trajectories, and therefore the likelihood of tracking, has been minimized.

Thanks to the applied RRM, the EMS is now more privacy-friendly to its users.

IV. CONCLUSIONS

Nowadays, a plethora of IoT platforms and solutions exist, but yet no large-scale and cross-platform IoT ecosystems have been developed. This is mainly due to the fragmentation of IoT platforms and interfaces, as this variety results in high market entry barriers. The BIG IoT project aims at establishing interoperability across platforms in order to ignite an IoT ecosystem. Core technological pillars of BIG IoT are a common API as well as a marketplace for all participants of the IoT ecosystem, including devices, end-users, and service providers. Key to its success is to define appropriate levels of security and privacy.

This work proposes an approach for identifying and rating privacy risks in the IoT domain. The approach is based on the OWASP risk rating methodology but adapted to the IoT domain. This is done by only selecting the most relevant

factors and also applying weights to the factors to further adjust them for the domain. The approach is exemplified by applying it to a typical IoT use case namely the Environment monitoring service. By applying the privacy risk rating methodology the various factors are evaluated for an identified risk. The overall risk severity is obtained based on the factor scores, which forms the basis for recommending remediation of the risk. The remediation consists of a number of recommendations for aggregating location data to areas and removing identifiers from the data. Furthermore, it is also illustrated how to integrate the risk rating methodology with the SDLC.

With IoT becoming more widespread and integrated as parts of big complex systems, the aspect of maintaining the privacy of data is more relevant than ever. In doing this, it is important to be able to identify and evaluate risks to privacy of data, which can be done using the proposed RRM. In the presented example it is shown that the approach can cover complex system setups, such as a use case in the BIG IoT ecosystem.

Future work includes applying the proposed RRM in more use cases, evaluating its applicability. While doing this it should be formalized how the remediation actions, which are the outcome of the RRM, should be included in the SDLC. Moreover, future integration with threat/vulnerability databases for the automated identification of IoT-related vulnerabilities should also be considered.

Acknowledgement

This work is financially supported mainly by the project Bridging the Interoperability Gap (BIG IoT) funded by the European Commission's Horizon 2020 research and innovation program under grant agreement No 688038. In addition, this work has been partially supported by the MINECO/FEDER funded projects ANFORA TEC2015-68734-R and ARPASAT TEC2015-70197-R and by the Generalitat de Catalunya grant 2014-SGR-1504.

References

[1] A. Bröring, S. Schmid, C. K. Schindhelm, A. Khelil, S. Käbisch, D. Kramer, D. L. Phuoc, J. Mitic, D. Anicic, and E. Teniente, "Enabling iot ecosystems through platform interoperability", *IEEE Software*, vol. 34, no. 1, pp. 54–61, Jan. 2017, ISSN: 0740-7459. DOI: 10.1109/MS.2017.2.

[2] J. Hernández-Serrano, J. L. Muñoz, A. Bröring, O. Esparza, L. Mikkelsen, W. Schwarzott, O. León, and J. Zibuschka, "On the road to secure and privacy-preserving iot ecosystems", in *Interoperability and Open-Source Solutions for the Internet of Things: Second International Workshop, InterOSS-IoT 2016, Held in Conjunction with IoT 2016, Stuttgart, Germany, November 7, 2016, Invited Papers*. Cham: Springer International Publishing, 2017, pp. 107–122, ISBN: 978-3-319-56877-5. DOI: 10.1007/978-3-319-56877-5_7.

[3] European Parliament, Council of the European Union. (Apr. 2016). Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation), [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679.

[4] Ponemon Institute and IBM Security. (Jun. 2017). 2017 cost of a data breach study, [Online]. Available: https://www.ibm.com/security/data-breach.

[5] A. Jacobsson, M. Boldt, and B. Carlsson, "A risk analysis of a smart home automation system", *Future Generation Computer Systems*, vol. 56, pp. 719–733, 2016, ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2015.09.003.

[6] R. M. Savola, P. Savolainen, A. Evesti, H. Abie, and M. Sihvonen, "Risk-driven security metrics development for an e-health iot application", in *Information Security for South Africa (ISSA), 2015*, IEEE, 2015, pp. 1–6.

[7] H. Tai, A. Celesti, M. Fazio, M. Villari, and A. Puliafito, "An integrated system for advanced water risk management based on cloud computing and iot", in *Web Applications and Networking (WSWAN), 2015 2nd World Symposium on*, IEEE, 2015, pp. 1–7.

[8] A. Arabo, I. Brown, and F. El-Moussa, "Privacy in the age of mobility and smart devices in smart homes", *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*, pp. 819–826, 2012.

[9] D. Kozlov, J. Veijalainen, and Y. Ali, "Security and privacy threats in iot architectures", in *Proceedings of the 7th International Conference on Body Area Networks*, ser. BodyNets '12, Oslo, Norway: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012, pp. 256–262, ISBN: 978-1-936968-60-2.

[10] R. H. Weber, "Accountability in the internet of things", *Computer Law and Security Review*, vol. 27, no. 2, pp. 133–138, 2011, ISSN: 0267-3649. DOI: https://doi.org/10.1016/j.clsr.2011.01.005.

[11] M. Meucci and A. Muller. (Apr. 2016). OWASP testing guideline version 4, [Online]. Available: https://www.owasp.org/index.php/OWASP_Testing_Project.

[12] OWASP. (May 30, 2016). OWASP Risk Rating Methodology, [Online]. Available: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[13] R. S. Ross, "Guide for conducting risk assessments", National Institute of Standards and Technology, Special Publication 800-30, version Revision 1, Sep. 17, 2012. DOI: 10.6028/NIST.SP.800-30r1.

[14] R. A. Caralli, J. F. Stevens, L. Young, and W. R. Wilson, "Introducing octave allegro: Improving the information security risk assessment process", Software Engineering Institute (Carnegie Mellon University), May 2007.