RELINK

Oslo Metropolitan University
Faculty of Technology, Art and Design

EUROPEAN PROJECT SEMESTER (EPS)

Group M

Caroline Gau
Eray Kip
Eren Sensoy
Edjinam Siliadin

August 2019 – December 2019

Institute for Information Technology
Post address: Postboks 4 St. Olavs plass, 0130 Oslo
Visiting address: Holbergs plass, Oslo
Phone: 22 45 32 00

PROJECT LETTER	
AVAILABILITY	

European Project Semester

MAIN PROJECT TITLE: RELINK	DATE 03.12.2019 NUMBER OF PAGES/APPENDIXES 54
PROJECT TEAM MEMBERS Caroline Gau (s339162) Eray Kip (s339166) Eren Sensoy (s339181) Edjinam Siliadin (s339185)	INTERNAL SUPERVISOR(S) Main internals: Terje Gjøsæter Anthony Giannoumis Supporting internal: Cristina Paupini

EXTERNAL SUPERVISOR Henry Mainsah	CONTACT PERSON

ABSTRACT

The major goal of the project was to build a model for risk assessment, a tool to measure the digital risks associated to smart devices. In addition, group M designed a process of development along with the assessment in order to support further developments and attempts to improve the current model. The group also provides the guide for using the model.

The overall structure of this report takes the form of seven sections. It first gives a brief overview of the context of this project, its purposes and to who it is addressed. After the introduction, it shows how the group has developed the project. Precisely, the management part and the process of the delivery. The third section presents the results, the final model and the guide how to use the model and to expand it. Section four discusses the results and the made decisions during the work. After that, the conclusion, including the summary of the project and recommendations for further work on our project. Next, there is the group reflection to show what added values and knowledge it has brought the group during the semester in the group work. At the end of this report, there are all the references used and appendices.

List of Contents

List of Figures and Tables

Abstract

Smart devices can perform autonomously a wide range of tasks on user's behalf. On the dark side, they are a major concern for network experts because these devices are designed for precise purposes regardless of all the existing ways to exploit them.

As standalone systems, smart devices represent only advantages for consumers whereas when they are connected, they are sources of digital risks the users tend to ignore. Integrated to a larger project initiated by Norwegian authorities, EPS project RELINK consists into providing tools and resources to identify the digital risks smart devices represent.

Our team reviewed the market of smart devices in Norway and met manufacturers and resellers to gather exclusive data about the Internet of Things and smart home devices state of the art. Furthermore, the major goal of the project was to build a model for risk assessment, a tool to measure the digital risks associated to smart devices. In addition, we designed a process of development along with the assessment in order to support further developments and attempts to improve the current model. Finally, we provide the guide for using the model.

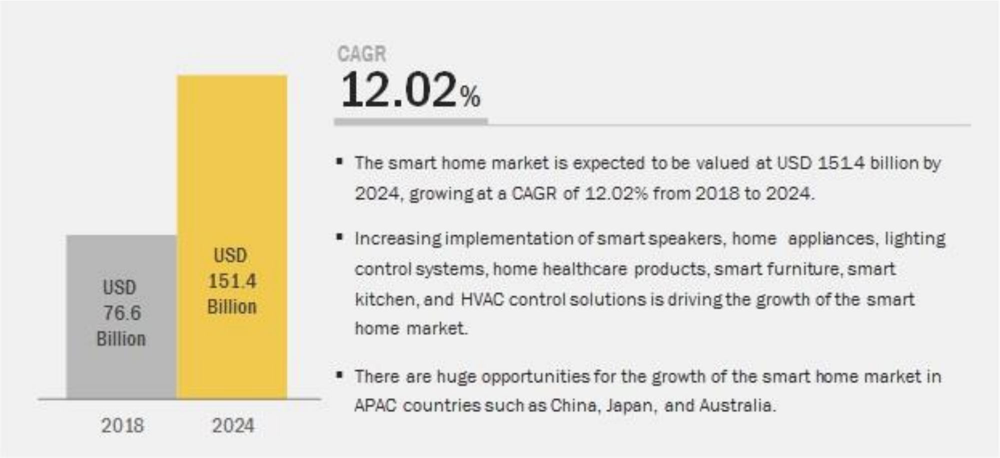
1 Introduction

1.1 Background

Smart Devices are intelligence-rich, electronic gadgets networked through the Internet of Things (IoT). They communicate via wireless protocols such as Bluetooth Low Energy (BLE), Wi-Fi, Near Field Communication (NFC) or cellular (Silverio-Fernández, Renukappa, Suresh, 2018). These devices are designed to capture information that they process and then transfer their results to other smart devices, such as a smartphone.

IoT describes the network of physical objects that integrate sensors, software and other technologies to connect and share data over the Internet with other devices and systems. These devices range from normal household appliances to sophisticated industrial tools. According to research from Strategy Analytics (2019), the number of devices connected to the internet reached 22 billion worldwide at the end of 2018. They predict that 38.6 billion devices will be connected by 2025, and 50 billion by 2030. “The IoT is a giant network of connected devices, or in other words, ‘Things’”. (Jacob Morgan, 2014).

A living space equipped with multiple smart devices is called a smart home. Smart home technology is intended to make everyday life more comfortable and efficient for consumers. This is also beneficial for the United Nation Sustainable Development Goals where they try to create a more sustainable future. Further information about goals such as responsible consumption and production or sustainable cities and clean communities that match our project can be found in the Project related to UN Sustainability Goals 8.1. The smart home market is expected to grow by USD 74.8 billion from 2018 to 2024, at a Compound Annual Growth Rate (CAGR) of 12.02 % (MarketsandMarkets, 2019).



- The smart home market is expected to be valued at USD 151.4 billion by 2024, growing at a CAGR of 12.02% from 2018 to 2024.
- Increasing implementation of smart speakers, home appliances, lighting control systems, home healthcare products, smart furniture, smart kitchen, and HVAC control solutions is driving the growth of the smart home market.
- There are huge opportunities for the growth of the smart home market in APAC countries such as China, Japan, and Australia.

Figure 1: Expected value growth of smart home market by 2024 (MarketsandMarkets, 2019)

1.2 State of the Art

The field of IoT and smart devices is large and complex. Within this field, work that has examined security issues is particularly relevant for this project.

In 2015, Abomhara and Køien published a paper in which they help to get an overview of the topic IoT. IoT devices and services and their security issues got explained by the authors. They also describe security threats, attacks and vulnerabilities. The paper has a list of primary security and privacy goals and gives an insight in motives and goals of cyber-attacks.
The authors point out that "there is a real need to secure IoT, which has consequently resulted in a need to comprehensively understand the threats and attacks on IoT infrastructure" (Abomhara & Køien, 2015)

A study investigated the major security and forensics challenges of IoT (Conti, Dehghantanha, Franke, & Watson, 2017). IoT is offering a very big network of objects that are interacting and exchanging data with each other. This gives cyber-attacks an ideal opportunity to get advantage of that, because of the stack of data IoT collects. The authors say that IoT environment is getting challenged by security issues such as privacy, access control, secure communication and secure storage of data. They conclude that "[t]he fast growth of IoT devices and services led to deployment of many vulnerable and insecure nodes" (Conti, Dehghantanha, Franke, & Watson, 2017, p. 544). The authors also point out that the identification, collection, preservation and reporting of evidences of cyber-attacks are very challenging the forensics.
This article is relevant for the project, because IoT is being developed at a very fast pace and that brings different challenges with it. The article shows different kinds of security issues and helps to understand them. To enlighten the consumers is one of the first steps to fight against these issues and start to overcome them.

Another article deals with the subject that technologies that intend to create new value and options concurrently increase vulnerability. Even new vulnerabilities arise as digital technologies attempt to solve these problems (Ransbotham, Fichman, Gopal, & Gupta, 2016).
As new smart devices are coming onto the market almost every day, the problem about their vulnerabilities they bring with is a very relevant issue for the project.

1.3 Problem description

Prior studies have noted the importance of increasing the security, because the IoT develops so fast and therefore brings a lot of risks with it. The problem here, is that the users are largely unaware of these risks (Apthorpe, Chetty, Feamster & Zheng, 2018). Also, the lack of education in the market about these security risks is a big problem (Chircu & Ahlmeyer, 2016). These problems of ignorance about the dangers and their education is what the group wants to address with the model.

1.4 Mission and Goals

This EPS project is a part of a larger program called RELINK, funded by the Research Council of Norway's IKT Pluss programme. The researchers are considering the current situation where household lack of good tools and resources to help them to identify and to evaluate digital risks related to smart devices (RELINK, 2019). EPS Group M participates in this large program with its works over smart devices in Norway.

The first job was to research smart devices to have an overview in the Norwegian market. Then, team needed to develop a model of a Risk Assessment capable of evaluating digital vulnerabilities smart devices are exposed to. Subsequently, the model developed can be re-used and perfected to become a relevant tool for the purpose of evaluating the vulnerabilities of smart devices. Final mission consisted into gathering opinion of experts working in the field of IoT regarding the state of the art and our initiative

1.5 Stakeholders

The project RELINK involved the EPS students in group M. Few external participants provided valuable guidance and their expertise to assist the EPS group and contributed to this project.

There are two different groups targeted. The primary target group is an audience with similar characteristics as the group M. This audience can be a group of experts, a club of IoT friendly students, individual skilled cyber-security consultants because some of the risk assessment questions require technical background to be taken.

This group of people may use our work in two ways. Either continuing to develop the model of Risk Assessment or using the model to analyse a device or a sample of them. This type of organisation can bring its talent together and simplify the model delivered after this project and make it even more accessible.

The second target group is consumers globally. These users are expected to evaluate their devices through the assessment and then to identify where they are exposed and what is the degree of exposure to potential dangers.

1.6 Structure of report

The overall structure of this report takes the form of eight sections. It first gives a brief overview of the context of this project, its purposes and to who it is addressed. After the introduction, it shows how the group has developed the project. Precisely, the management part and the process of the delivery. The third section presents the results, the final model and the guide how to use the model and to expand it. Section four discusses the results and the made decisions during the work. After that, the conclusion, including the summary of the project and recommendations for further work on our project. Next, there is the group reflection to show what added values and knowledge it has brought the group during the semester in the group work. At the end of this report, there are all the references used and appendices.

2 Project Development

2.1 Organisation

2.1.1 Meetings

The group decided to meet at least three times a week in order to keep up to date and work constantly. Since all group members stay in the same student housing, the location of the meetings was in a cafe near to the student housing. In addition to the private meetings, the group arranged a weekly meeting with the supervisors, to show them how the project was progressing and to receive feedback.

2.1.2 Project Management Software

Our group used different tools to organize and plan the work and documents for the project. Some of these tools were Monday, Trello, Miro, OneDrive.

To get an overview of the various tasks, the tools Monday.com and Trello.com have been used. The tasks were divided into the sections to-do, ongoing, done and stuck and into group work and individual work.

All documents were uploaded to a shared folder in OneDrive. This meant that all documents created were in one place so that each member could edit and view the document at any time.

For brainstorming and mind mapping our group used the software Miro.com. As the group began with a new theme or idea, the Mind Map helped to collect all the ideas, plans, and concepts of the members and discuss the outcome.

2.1.3 Role Allocation

We agreed to use the concept of changing role allocation. That means that every member had a role as leader, tech, researcher or writer that changed weekly. The aim of this concept was to force every member to do different work, especially in areas that they are less confident in volunteering for. This helped to give all members a clear path to participation, promote individual accountability and to strengthen our communicative skills.

2.1.4 Challenges

Over time, the group has encountered various problems and challenges. When the group had conflicts with each other, it was important to talk to each other and resolve these disagreements. When we did not get an interview with a big company, we did not give up. We have also contacted other companies and decided not only to conduct interviews with companies, but also with a group of experts. The delivery of the project was a difficult topic for the group. At the beginning, there was a different idea of the delivery than towards the end of the project. Besides these examples, there were many other challenges the group faced. However, the group was able to clarify everything, and a solution was always found.

2.2 Process

2.2.1 Overview of Smart Devices

For the process in the beginning, the first step to start was to get an overview about the existing devices available in Norway. The research on various devices had to be done on the internet and in local shops. The devices are used in different places in the house, such as the living room or the kitchen. Each group member searched for every possible kind of device in these places. To get a better comparison of these devices among each other, two different products per device were selected. The list of all devices can be found in the Overview of Smart Devices available in Norway 8.2.

Close related to smart devices, the concept of smart homes was checked during the group researches.

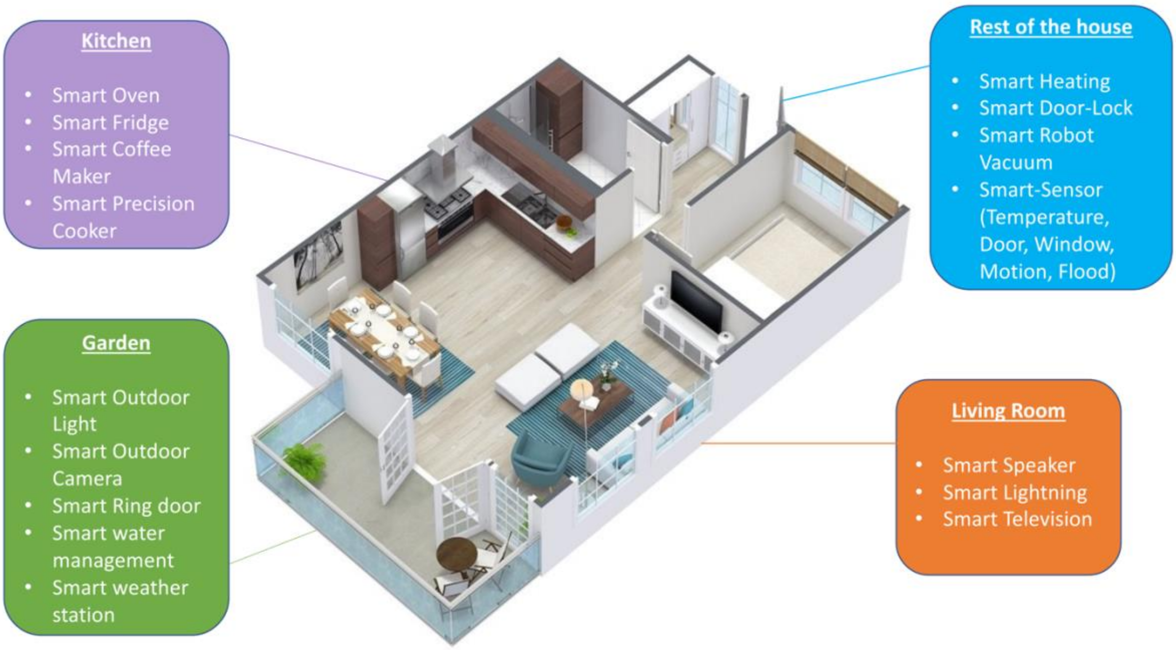


Figure 2: Positioning diagram

As known, a house where multiple smart devices are implemented is a smart home. These enhanced habitations are full of small to larger smart devices from sensors families to larger systems. Though, all the devices are required to work together in order to provide the best service and experience to the user. Hence, the smart devices are connected one to another in the smart homes. Right below, find a connection diagram the team designed with the output of the researches.

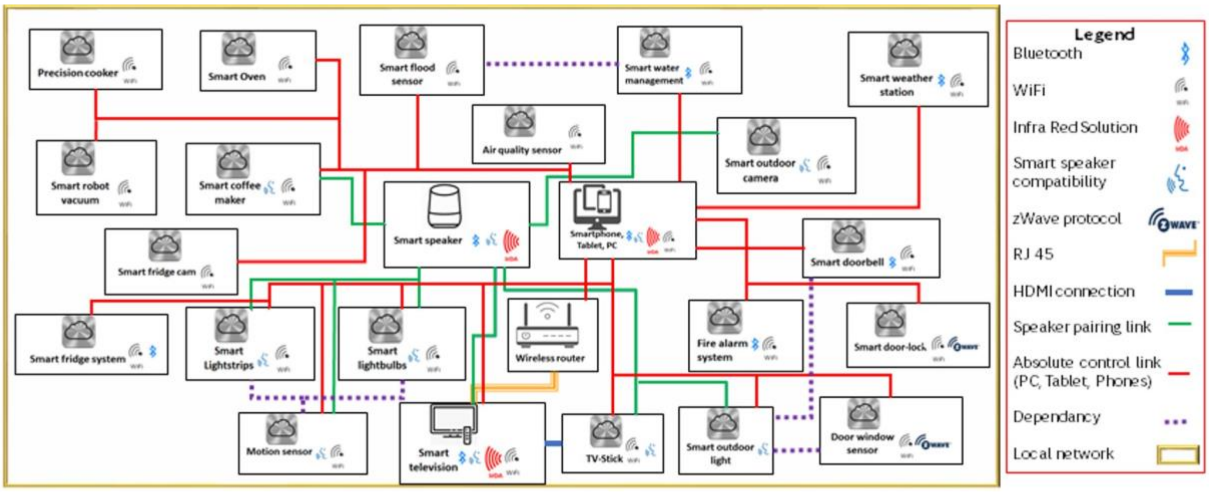


Figure 3: Connection diagram

This diagram is very complex and it may be difficult to read. First, there are many smart devices in a smart house, furthermore multiple connection method used. But this also explains why there are so many weaknesses in the smart houses. Every device is potentially a weak point inside the network. However, every communication means there is data flow. For users this analysis is not easy to accept nor to understand but it is real: This is IoT with its benefits and its drawbacks.

2.2.2 Developing first Risk Assessment

The decision to develop a risk assessment came after the second meeting. Initially, the idea was to develop a risk assessment that compared devices within the same family of devices in order to evaluate their degree of safety. Knowing that there were a certain number of smart devices to evaluate, a maximum number of 10 assets was defined. Along with this decision, the way to grade the devices was fixed as follow.

- Every question is graded with one point.
- Devices are marked from 0 to 10 as from lower to higher “risk-friendly”.
- Triggers were decided also to provide visual badges to devices:

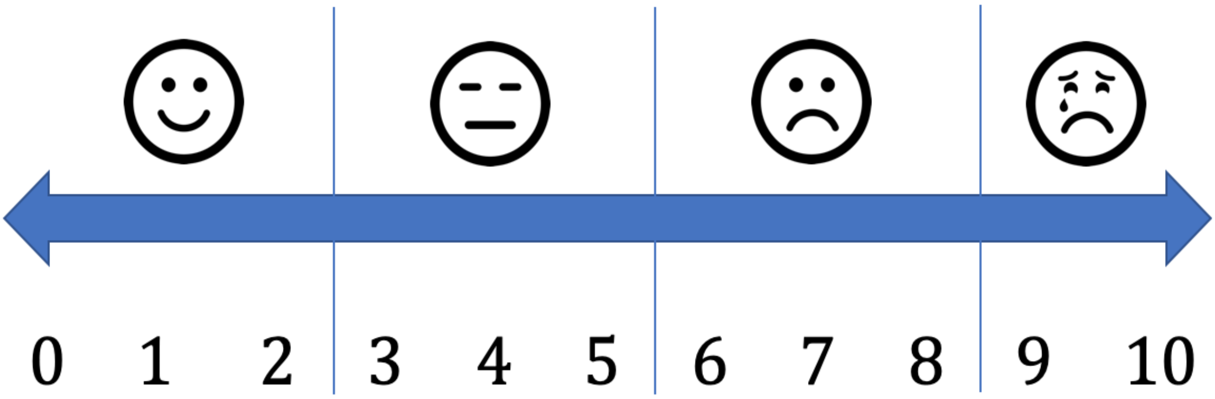


Table 1: Meaning of the grades

Every group member was requested to bring ideas through a brainstorming. These were whether relevant questions that evaluate strictly a security weakness or imagined scenarios of attacks. This process required three days brainstorming too and one day to pick the best options and to fix the sentences.

Find in First Risk Assessment 8.3.2 the questions and results of the first Risk Assessment

2.2.3 Results of first Risk Assessment

The first version of risk assessment was made in order to compare the families of smart devices one to another and to observe the tendency of the market. Apart from a few exceptions, most of the devices had similar grades. These results display the tendency of manufacturers to follow official standards. Furthermore, a few devices got low grades due to very little improvements or a clear communication, such as the smart speakers. On the other side, devices like the smart fridgecam got higher risk grade because the manufacturers released very little technical information's.

After every device got passed through the risk assessment, different results have been made. To visualize these results, several diagrams were created.

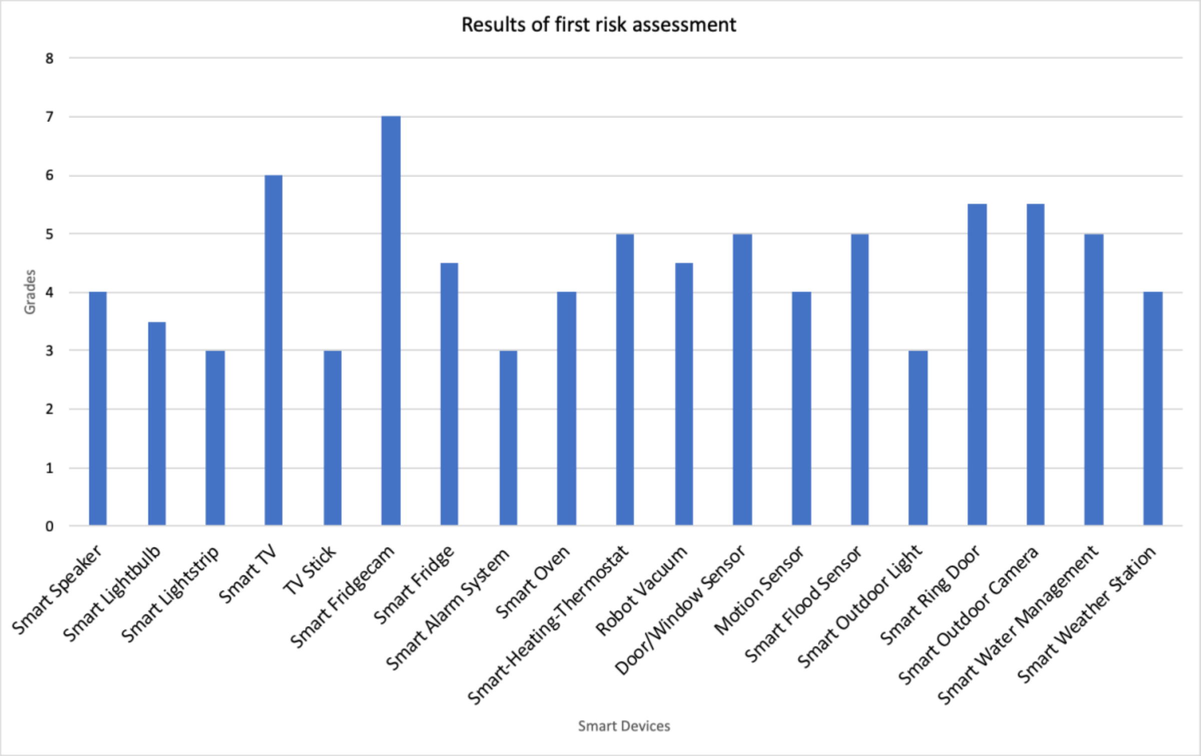


Figure 4: Results of first Risk Assessment

Figure 4 provides a visual output of the first risk assessment to present the results in a graphical perspective.

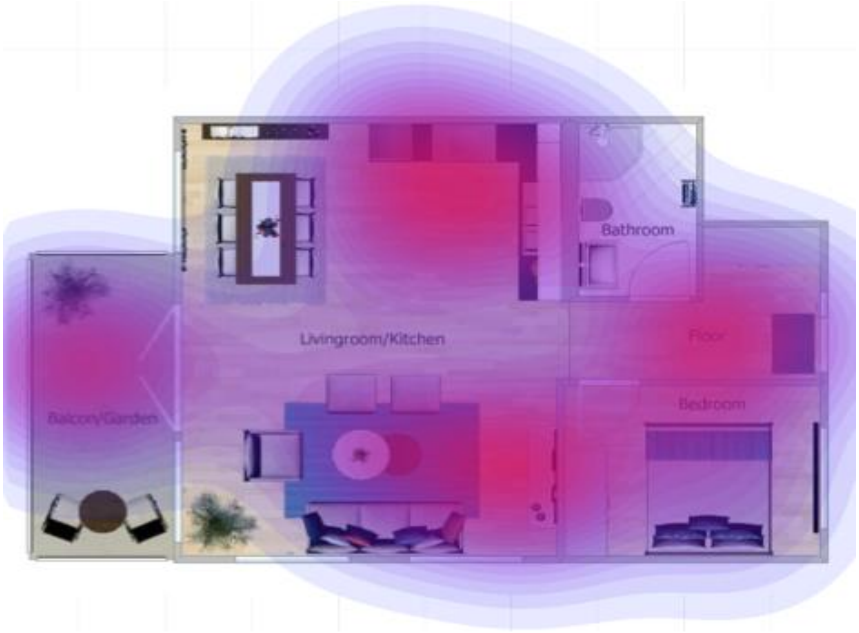


Figure 5: Heatmap

The heatmap shows the concentration of risks in the house based on the evaluation of the devices.

2.2.4 Redefinition of the project's goal

As required when the project began, our team had to scout the market in Norway and find out what smart devices are available. Individually every group member knew different smart devices, but they were not all commercialized in Norway. The second part of this project consisted into reporting the risks related the available smart devices found.

Not less than Seven countries in UE, including Norway, notified their national data protection organism Google's violation to GDPR terms by tracking users (Maack, 2018).

Understanding the trends and the way manufacturers are running their business, the group realised the importance of its enterprise. The first version of the risk assessment questionnaire was designed by the team for internal use. All the participants of the project acknowledge that this type of method of evaluation was a valuable thing. This type of process did not exist in a user-oriented version. Furthermore, due to a need of transparency in the results from our works, the process was as important as the results of our survey about the risks related to smart devices in Norway. Thus, the team decided to change its perspective. Instead of making a survey about the risks related to smart devices in Norway, the project changed its goal to providing a flexible model to evaluate the risks related to smart devices: The Risk Assessment Model.

2.2.5 The cycle of development

The first version of risk assessment was made and oriented to satisfy a single audience; the project group. The initial need to gather a maximum information, to figure out the risks related to smart devices in Norway inspired this work. Its major objective was filled. However, this assessment did not satisfy our team due to the subjectivity of couple questions, to a lack of data from many manufacturers, and finally, to the other questions it brought up.

It was therefore clear that the process had to be repeated with new and refined questions in order to get a more accurate and general results.

Interviews made with professionals of IoT field confirmed these observations. Reviews of these interviews are available in theInterviews

And this type of repetition and improvement will and must be done in the future too, so that it can be ensured that the risk assessment and model always remains up-to-date and can be adapted. The guide how to extend the model will be demonstrated later in the report under section three results.

2.2.6 Final Risk Assessment

Two factors led to a further work over the risk assessment model. The first was a lack of depth in the assessment's themes. This was wanted in a first place but was an accurate source of critics if an outside source would evaluate the project. Moreover, the project evolved and required a solid outcome. From these two aspects, the risk assessment was remade over and over through the cycle process explained before. Thanks to the previous analysis, the limits of the elder versions were underlined, therefore the work consisted into going deeper in the questioning and exploring further options such as legal aspect with the Global Data Protection Rules (GDPR). The future point to improve in the risk assessment model is flexibility to address the wider audience possible.

The team brainstormed alongside with the supervisors proceeded to tests then built a final version of Risk Assessment. This final version represents the major accomplishment of this project. It is delivered along with a How-to document in order to allow anybody to proceed. Details are developed further in this report.

2.2.7 Results of final Risk Assessment

This final version of Risk Assessment was performed over a sample of 4 families of smart devices taken from different locations of the house: Smart speakers, Smart Lightbulbs, Smart Fire Alarms system and the Smart outdoor cameras. Three devices were analysed in each family in order to point a tendency or on the contrary a difference in the manufacturer's vision. The diagram output allowed us to develop the following analysis.

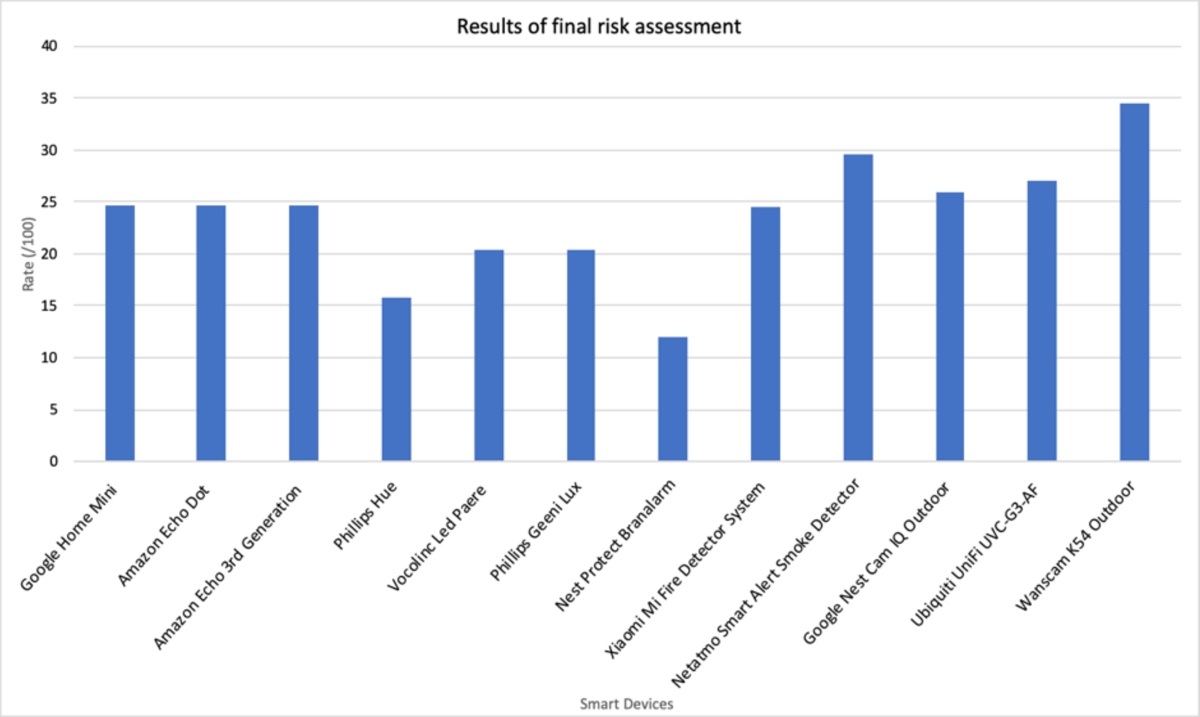


Figure 6: Results of final Risk Assessment

Smart speakers family of devices follow similar policies and use the same technologies in term of security. As a result, the grades of these devices were the same. On the other extreme, limited to this precise sample, Smart Fire Alarm detectors present very different grades from a device to another.

There is no global tendency in the market regarding specific family of smart devices. It is whether the segment respects the same optimization or from a manufacturer to another, the vision is different. They choose to whether optimize the price of their devices or the functionalities related or the equipment's security.

From this sample, the grades stayed between 15/100 to 35/100. The fluctuation is very limited but remains worth an analysis considering that chosen devices are at different zones perform very different tasks. Although, the grades increase mainly due to a lack of information from the manufacturers.

When the products are made by big companies, consumers are flooded with a maximum information. These giants possess structured websites with various sections where it is possible to access the key data to answer the assessment. Unfortunately, custom or small manufacturers do not have this privilege. Therefore, many questions remain unanswered.

3 Results

The results of the project are the model, consisting of the final risk assessment and the guide to be able to answer the questions and in addition how to develop the model.

3.1 Final model

3.1.1 Presentation of the questions

1. Is the device connected with other smart devices?

    1.1 Wired

    1.2 Wi-Fi

    1.3 Is it possible to connect it to 3G, 4G, 4G+, 5G?

    1.4 Are there different connection/communication protocols available on it (Bluetooth, IrDA, Z-Wave, etc)?

    1.5 Does this device control other devices?

2. Does it use a custom network for initial configuration?

3. Is the data transmission over internet in clear text?

4. Does it generate/record/collect any private data?

5. Does it stream or upload data? (Even local-only streaming is dangerous)

6. Is the authentication uncontrolled? (ID/Password in the App is accepted)

    6.1 Does the manufacturer force to change the default password and login? (Answer no is a danger)

7. Does it use multiple factors method for authentication? (Answer no is a danger)

8. Is the OS based on unknown kernel?

9. Does the current version of the OS have known vulnerabilities?

    9.1 Are software upgrades & security patches applied automatically? (Answer no is a danger)

9.2 Can up-to-date OS versions or release notes easily be found? (Up-to-date means last update or patch was included during the past 9 months.) (Answer no is a danger)

10. Is the device designed to be controlled from a remote network?

11. Are there system logs?

11.1 Are they stored on cloud?

11.2 Are they in clear text?

12. Do the manufacturer collect personal data?

12.1 Does the company claim to follow GDPR's requirements? (Answer no is a danger)

12.2 Is personal data shared with third parties (even partners)?

13. Are user information and operational data merged?

14. Is the end user licence agreement published? (Answer no is a danger)

14.1 and if so, does it include security guide or notes & warnings? (Answer no is a danger)

15. Grades:

15.1 Rate from 1 to 5 the potential impact of a data breach/leak from this device. (1 low impact -> 5 high impact)

15.2 Rate from 1 to 5 the physical impact of a malfunction or a defect of the device. (1 low impact -> 5 high impact)

3.1.2 Description

The final version of Risk assessment is a developed series of questions exploring multiple characteristics of smart devices. The first questions (Q1 – Q3) check device's connectivity by exploring the protocols used for its connections to local network and distant connections. Besides, data transmission is analysed to verify if encryption mechanisms are enabled (Q4 - Q5). After these, the risk assessment questions the authentication to the device (Q6 - Q7) then moves onto an overview of the Operating System information along with its update procedures (Q8 - Q9). The next steps concern data storage, data protection guarantees and end user license, guide & procedures (Q10 – Q14).

The questionnaire ends with a subjective open question made to estimate the impact of an accident caused by the device over the house and on its owner, from the risk analyser's point of view.

3.1.3 Risks assessed

During the entire project, the team based its technical development over worse scenarios imagined by the group members from their individual experience. These are examples inspired from education courses, movies, literature and the experience from previous cycles of the Risk Assessment's design.

The multiple questions and sub questions aim to verify if the device prevents these 3 risks for the user:

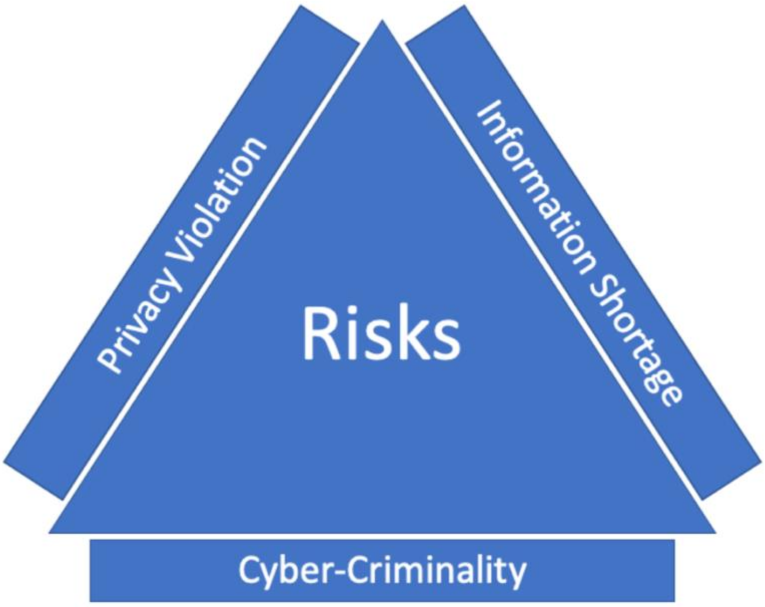


Figure 7: Three major risks

3.2 “How-to” - The support document

3.2.1 Capital gain of this document

The risk assessment model claims the ambition to be usable by anyone. This is where the guide’s importance is underlined. As well as explaining more precisely the meaning of every questions, the “how-to” document guides the user to reproduce a similar work without needing further assistance. On top of this point, every known evaluation process or scientific method comes with a recipe.

Through this document, the expert team describes the scheme to assess smart devices from a user point of view. Beyond this point of view, RELINK project group delivered an extended guide to assist a future attempt to build the next version of the Risk Assessment.

3.2.2 Presentation of the guides

The “how-to” document exists in two versions like mentioned in the previous section. It consists of a user only document for the first one and a user-tech document for the second.

The first is a strict guide explaining the steps required to take the risk assessment in the same way as its designers made it. As for the second one, it is a document that adds to the simple user guide details and specifications over the origin of the questions adopting a visual perspective through a diagram. Further in the report, our team provides sources to deepen in the future cycles of development. All these little “plus one” information is provided to encourage further development of this model.

The guides are support documents, inhering drawbacks of the technical assessment. They were considered necessary because, they explain the questions written in complex structures. Another example, sometimes the theme of question was too rich technically and this caused difficulties to provide clear explanations.

Guide for the Risk Assessment:

It is recommended to proceed to this evaluation individually and to gather and finally globalize the results. If you do not have the possibility to work in a team to work with, note that individual errors might occur and won't be detected.

- Every question requires a yes/no answer except question 15.1 and 15.2
- Answer the questions clearly and if you cannot find an answer, leave it blank.
- When a question is unanswered it will be interpreted as risk and graded consequently.
- Every time the answer is "Yes" it means there is a danger except when reverse is mentioned after the question.
- List the sources you used to answer the questions for every device.
- The sub questions are made to precise the major question.
- If a question has sub questions, grade the sub questions before main one.
  (For example, to say if a device is connected, we need to check the 5 sub questions and then we divide the point for question 1 by the amount of connection options that matches.)

- Question 15 are here to underline the degree of exposure. We assume a smart vacuum cleaner and a smart camera don't have the same possible impacts. One can probably release house's plan modelized from its sensors whereas the other can directly show what is where and who is where. In this case vacuum cleaners 15.1 grade could be 3 whereas camera's 15.1 grade be 4 or 5 depending on its location.
- Rating the possible risks multiplies the overall result and balances grades between all the devices.
- After merging and verifying the results it is time to grade the devices individually. (May need to view the sources here)
  Note that regarding question 15.1 and 15.2, you need to make an average within the outputs.

- The final mark is determined by summing the marks of principal questions from 1 to 14 and multiplying this number by the sum of question 15.1 and 15.2 grades.
- Bring the total result to a scale from 1 to 100.
- Additional feature is to check the percentage of questions unanswered.

Guide to extend the Model:

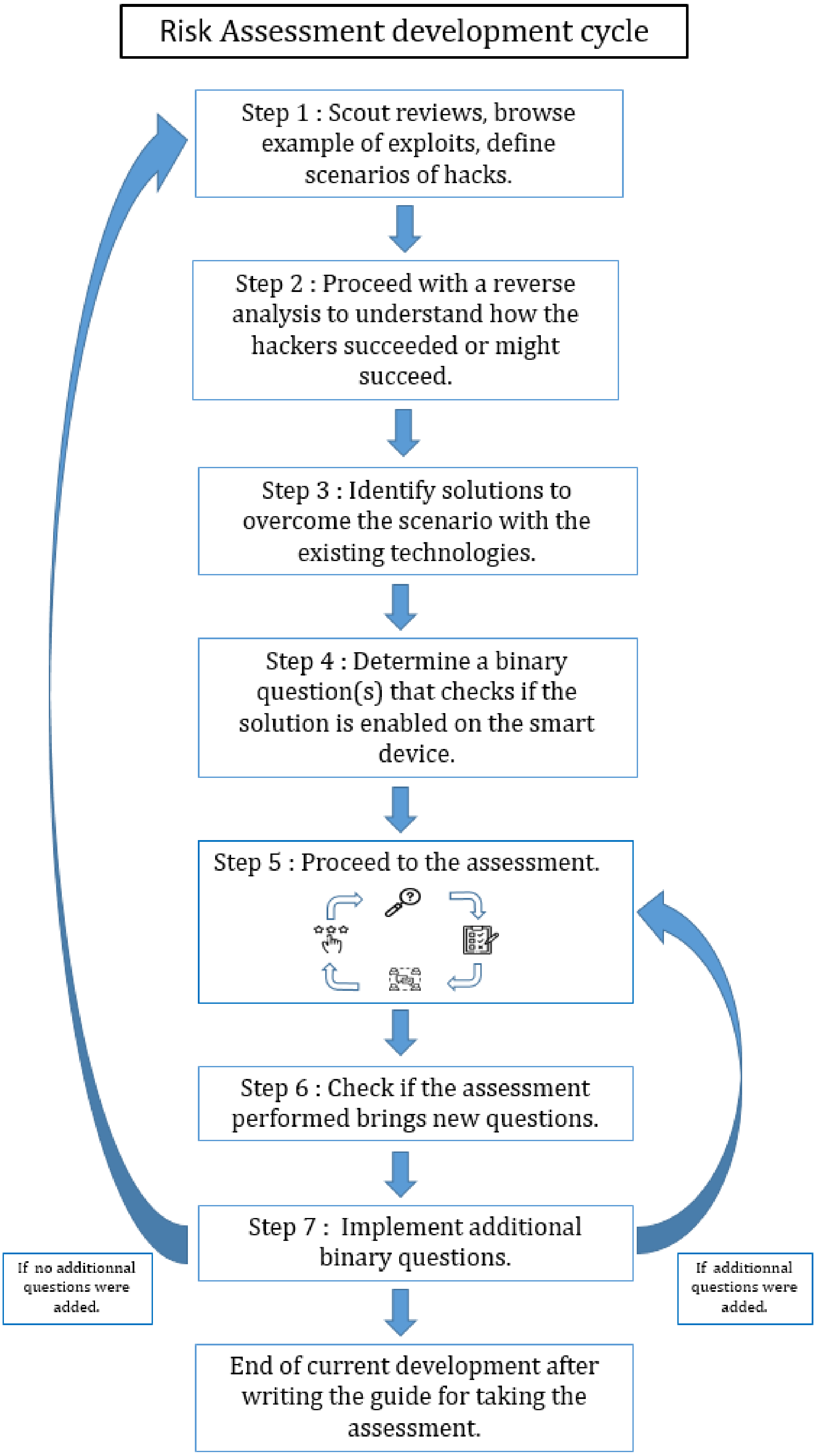

Risk Assessment development cycle
Step 1 : Scout reviews, browse example of exploits, define scenarios of hacks.
Step 2 : Proceed with a reverse analysis to understand how the hackers succeeded or might succeed.
Step 3 : Identify solutions to overcome the scenario with the existing technologies.
Step 4 : Determine a binary question(s) that checks if the solution is enabled on the smart device.
Step 5 : Proceed to the assessment.
Step 6 : Check if the assessment performed brings new questions.
Step 7 : Implement additional binary questions.
End of current development after writing the guide for taking the assessment.
If no additionnal questions were added.
If additionnal questions were added.

Figure 8: Risk Assessment development cycle

3.2.3 Grades

The process of grading the devices post-assessment is described inside the guide also. After designing every version of the Risk assessment, the team worked on shaping the outputs of the results for each device individually. They were represented with a rate number between 1 to 10, emotes and diagrams in the elder versions of the model. Regarding the final version, team members decided to quantify the degree of exposure, consumer faces when he/she uses the concerned smart device. This matter is measured on a percentage scale. This method's advantages are:

- Improved accuracy.
- More convenience for users.

As well as for the previous version, we kept the diagram to provide a graphical representation of the results.

4 Discussion

In the discussion part the strengths and critics about the model will be discussed. Subsequently, the groups choices and their significance are described. Finally, the first model is compared to the final model to show their differences.

4.1 Discussion of the results

The problem we wanted to solve with this project was the unawareness of the users about the risks related to smart devices/IoT and the missing education about that. Therefore, we developed our model to make people aware of these problems. Our project is in line with previous researches that have been mentioned in the State of the Art in which they issue the security problems in the field of IoT. Since our goal was not to solve the security issues, we tried to find a different solution by creating a model to assess smart devices in terms of risk. The advantages of this are that the model can be expanded at any time by experts and thus remains current. As a result, it can be applied at any time to the daily new appearing smart devices.

On the other side, the model could be too complicated for people without knowledge about smart devices because some of the questions require a certain amount of knowledge. Easier question could make the assessment more useable for everyone, but it would lose a lot of content and accuracy. Another critical point of the model is that fifteen questions could be not enough to get precise results, because not every topic can be fitted in fifteen questions. The limitation of the number of questions prevented the assessment to go more in depth.

4.2 Choices and their significance

The major decision in the project was to define a final delivery different from the original plans. After identifying the smart devices market in Norway, the team decided to analyse them individually. There was no existing process to perform this task, thus we developed our own method of assessment. After realizing how valuable this process was, we decided to push the work further and to modify our delivery consequently.

This decision triggered other ones with likewise importance, such as the increase in the number of questions, the introduction of sub questions to narrow the scope of the performed analysis. These decisions were necessary because they allowed us to deepen our model and make it more accurate.

Lastly, question 15.1 and 15.2 were the most difficult to justify. However, smart devices may provoke higher or lower damages on user and the house physically. This aspect needed to be addressed in a way or another.

The last important decision we made was to define two different target groups:

- The first group is teams of experts or organizations concerned by user's security.
- The second is consumers of smart devices, just as demanded initially.

Group M created a model to assess smart devices and wishes to publish this model to leave it accessible to anyone. Starting from this version of Risk Assessment, experts can continue developing the process based on our works and using our methods. We provide then specific guidelines to help this type of challenge.

4.2.1 Scope of risks

This project's concern goes further than the global lines of systems security (Authorization, Authentication and Accounting) as cyber-criminality acts beyond user interface's limits.

This risk assessment does not check all the possible vulnerabilities. Every day, there are other methods and exploits revealed. To make this model reach the requirements of the state of the art, more cycles of development are needed. There cannot be a perfect model defined because hackers will identify and reveal new vulnerabilities, then develop alongside techniques to perform their exploits. In IT and security, there is no limit. The security methods, triggers, policies, (…) need evolve permanently.

4.2.2 Scale of grades

For the first risk assessment, each device was graded from 1 to 10. This scale was intuitive because there were 10 questions. So, 1 point was attributed if it was considered risky for each question or 0 otherwise. The results were not precise, some devices were riskier than others regardless the role the devices have in the house. To illustrate the case, the smart fridgecam was riskier than a smart speaker from the partial and basic evaluation method we developed. This result was questionable in different aspects. Firstly, the fridgecam is a device taking pictures of what's inside the user's fridge and sends the picture to an app. Besides these functions, it cannot do anything. Regarding risks, this device exposes the end user exclusively to cyber-criminality threats. On the other side, other devices such as smart expose the user to the three major risks (Privacy violation, Cyber-Criminality, Information shortage) our team analyses, but are still graded safer. More examples are available in the results of the first risk assessment model. Find this document in First Risk Assessment.

Therefore, the group decided to make deepen its model. The new risk assessment required more questions but also a new method to establish the grades. From the first question to the fourteen, 1 point was attributed. Some questions may have sub questions. The sub questions were very accurate and points specific situation, configurations, technologies, or details. In the context of sub question, the global point affected to the main question was divided by the amount of sub questions. Then all the points were added. Questions 15.1 and 15.2 are multiplying factors. These questions evaluate the impact of hacks, malfunctions or data breach over the house or over the user's life. These factors brought a streamline to the results observed through the assessment. Final grades are brought to a scale from 0 to 100. A larger scale to view smaller differences. The team named the grade rate of exposure.

4.3 Comparison of first and final Assessment

From a tool to help us to make a report about smart devices in Norway, the Risk Assessment Model became the delivery of the entire project we have conducted. The difference is immense. Therefore, differences exist in multiple aspects:

Aspect	Version 1	Version Final
Target group	Group M/Public	IoT-friendly people
Format	Yes/No questionnaire	Yes/No questionnaire with exceptions
Limitations	10 questions	15 questions with sub-questions.
Support document	Guide for the process	Presentation document, guide for process with examples, additional support process document
Evaluation	1 to 10 grades separated into four categories.	1 to 100 rating in percentage the degree of exposure.
Technical depth	Conceptional	Advanced (with the sub-questions, the intermediate versions, etc.)
Delivery	List of evaluated smart devices	Final model of risk assessment

Table 2: Comparison of first and final risk assessment

5 Conclusion

5.1 Summary

Team RELINK designed a model to measure the digital risks associated to smart devices through an experimental process. From a pilot version initially made to support the group's analysis, we came to the final version, presented as the main outcome of the entire project. The final version of Risk assessment is made for the use of people with likewise IoT knowledge or in a wider range, people who are ready to make deep researches to find answers to the questions. On the other hand, we acknowledge the model delivered does not meet all the objectives we fixed. To go further, here are recommendations for improvements of our model.

5.2 Recommendations for research

The risk assessment model is made of 15 questions that allow the group to define if the smart device is risky. Currently, the model is too complex for users without basic technical knowledge. The first improvement of the current risk assessment is to build even more questions in order to have a more complete version. Moreover, we recommend improving the flexibility of the guide in order to ease the model's use. A way to achieve these improvements are to meet with experts of the field and collect their ideas in an open discussion.

Generally, the companies claim to follow GDPR rules, but it is not always the case. According to the article from Marketingland, Google is accused of circumventing the GDRP's rules by enabling non-consensual data transfers with hidden push pages (Sterling, 2019). The recommendation here, is to find why some companies are accused of not following the GDPR despite the consequences of their behaviours on their own consumers. Therefore, a sub question in the privacy violation assessment can check whether the company is accused of GDPR violations for example.

5.3 Recommendations for practice

The risk assessment model is not published. For the next step, it would be a good idea to share it online by creating a website. Ideally, the users should be able to access it directly with a link. They would have to choose the smart devices family corresponding to the one they wish to evaluate. Then, provide answer the questions and they will get the results instantly. According to that, the website would give recommendations on how to protect their smart devices. The website could also have a statistic part with all the user's results collected.

Moreover, an app version could be created, making it easier to access the model downloading it from an app store (Apple store for example).

Finally, create a survey of the users to allow the group to bring some modifications on the risk assessment aspect, website or app at the end of each evaluation. This will allow to have different point of views.

6 Group Reflection

The European Project semester has been a new experience for us. We had never worked in an international, multidisciplinary group before.

Our group consisted of two German and two French students working on a project in English. Because of the language barrier we had to make efforts in order to understand each other in the first weeks. But after while we all improved and managed to communicate properly and exchange all our thoughts and ideas we had without any problems.

Different knowledge levels about the topic affected the understanding of the project and everybody had different capabilities which were not always properly used. However, everyone found the role in the group and provided to have an impact to the project.

The meetings with the supervisors helped us when we had problems and were stuck on different points. They always had wise words to enlighten us and to help us focus on the important tasks we had to do.

However, we sometimes had the feeling that our supervisors had different views, which confused us. This also occurred because we unfortunately could not often meet with both supervisors in a meeting.

On the bright side, we could often meet between us thanks to our location at Kringsjå student village. The odds were on our side on this aspect.

We gained experience in working with tools to organize ourselves. Scheduling and idea collection could be better handled. At first, we had very few different tasks on, therefor we did not need any software to keep a tracking of the jobs. Later, multiple tasks appeared in the calendar and we decided to use the software Trello after a quick try on the website monday.com. Monday was unfortunately not charge free.

In some weeks we had a low workload concerning the project because of a lack of motivation, or assignments related to the support courses to hand, but we still managed to finish everything in time and in a proper way.

The EPS was a profitable experience for team building and group working. Over time, we have been able to identify our mutual strengths and weaknesses and thus have been able to better distribute tasks. This project was a chance for us to get in touch with experts of the IoT and cyber-security market in Norway.

All in all, we are happy to have an even bigger outcome than the goal we set us in the beginning. It was a nice experience for us to work in a multi-disciplinary group. We learned a lot for our future life, and we would recommend it to everyone to participate at the EPS in Norway.

7 References

Abomhara, M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65-88.

Ahlmeyer, M., & Chircu, A. M. (2016). Securing the Internet of Things: A review. Issues in information Systems, 17(4).

Apthorpe, N., Zheng, S., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. Proceedings of the ACM on Human-Computer Interaction, 2(CSCW), 200.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems 78 (2018) pp. 544–546.

Maack, M. M. (2018). 7 EU countries accuse Google of violating GDPR by tracking users. TNW.

MarketsandMarkets (2019). Smart Home Market by Product (Lighting Control, Security & Access Control, HVAC, Entertainment, Smart Speaker, Home Healthcare, Smart Kitchen, Home Appliances, and Smart Furniture), Software & Services, and Region - Global Forecast to 2024. Market research report

Mercer, D. (2019). Global Connected and IoT Device Forecast Update. Strategy Analytics.

Morgan, J. (2014). A Simple Explanation of 'The Internet of Things'. Forbes Magazine.

Ransbotham, S., Fichman, R. G., Gopal, R., & Gupta, A. (2016). Special section introduction—ubiquitous IT and digital vulnerabilities. Information Systems Research, 27(4), 834-847.

Silverio-Fernández, M., Renukappa, S., & Suresh, S. (2018). What is a smart device? -a conceptualisation within the paradigm of the internet of things. Visualization in Engineering, 6(1), 3.

Sterling, G. (2019). Complaint alleges that Google is circumventing GDPR with RTB personal data sharing. Marketing Land.

8 Appendices

8.1 Project related to UN Sustainability Goals

UN Goals

The Sustainable Development Goals are a call for action by all countries to promote prosperity while protecting the planet. They recognize that ending poverty must go hand-in-hand with strategies that build economic growth and address a range of social needs including education, health, social protection, and job opportunities, while tackling climate change and environmental protection.

In our everyday life there are multiple actions we can do to contribute into reaching the different goals which are mentioned in the UN 17 goals. Being individually responsible of our carbon print on the earth is an ideology that has grown fast in the last few years and this start in our most private area, our personal office, our apartment and our houses.

RELINK & UN goals

The project RELINK consists in a deep analysis of what is going with smart devices on the end user's security aspect. Even though we are trying to figure out discriminant issues with the smart devices, our point is to promote those and to contribute in a process to overcome the risks identified.

Our actions may encourage people who do not trust these smart devices to try them with the guarantee that people looked deep into them and can attest that they are clean.

On the manufacturers point of view, it is also relevant to know what the current problems about smart devices are. They can therefore figure out the opportunities on the market and fill the empty spots.

More especially, we identified three relevant UN goal concerning our project more or less.

Goal 12: Responsible consumption and production is the most relevant. Known that smart devices are made to assist and to free the user from some basic tasks. As fact, these tasks are turning light down when there is nobody inside, closing the tap to not waste energy, managing heater to not waste energy heating unexploited rooms, and more. On the behalf of the end user, the smart devices are exploited to save energy and resources which is exactly what the united nation target as a goal in this situation. A financial aspect can be seen here, saving energy means saving money. For example, due to the low energy consumption of the smart devices like the lightbulbs, the end user uses less electricity so he will get lower bills.

As an addition, Goal 7: Affordable and clean energy" is our second goal associated. Smart devices like smart lightbulbs or smart lightning contribute to limit global warming. These technologies, allow the end user to control them from an app. By reducing their intensity or switching them off fast, it contributes to the reduction of the carbon emission. Moreover, they can warn people about the air quality if the home has an unhealthy air or not, by changing the light colour. So, they can change their ways to live in manner to be environmental-friendly.

As a third goal related to our project, we have picked Goal 11: Sustainable cities and clean communities. Actually, as smart devices' use can be extended everywhere in our cities to make them more responsible. As so we can have motion sensors in the streets related to smart lightbulbs that will enlighten the roads only when someone is walking there but will allow lights to be turned off if nobody is there. Developing this kind of smart cities would be helpful for the countries where there are often lack of energy or of resources such as water to control them.

8.2 Overview of Smart Devices available in Norway

Control Units			
Device	Example 1	Example 2	Example 3
Smartphone	 Apple iPhone 11 Pro 11990 NOK Apple.com/no	 Samsung Galaxy S10 9490 NOK Samsung.com/no	 Huawei P30, 6999 NOK Telenor.com
Tablets	 Apple iPad 3990 NOK Apple.com/no	 Galaxy Tab S6 7490 NOK Samsung.com/no	 Acer Chromebook Tab 10 2990 NOK Komplett.no
Smart watches	 Apple Watch 5 4690 NOK Apple.com/no	 Samsung Galaxy Watch Active2 4790 NOK Samsung.com/no	 Garmin Vivoactive 3 Music 2845 NOK Elkjop.no

Table 3: List of Smart Devices for Control Units

Living Room			
Device	Example 1	Example 2	Example 3
Smart Speaker	 Google Home Mini, 399 NOK Elkjop.no	 Amazon Echo Dot 454 NOK Proshop.no	 Amazon Echo (2. Gen.) 1390 NOK Power.no
Smart lightbulbs	 Geeni Lux 99 NOK Elkjop.no	 Philips Hue 460 NOK Elkjop.no	 VOCOLINC LED PÆRE 6W/E27 349 NOK Power.no
Smart lightstrips	 Yeelight LED Lightstrip 1m 179 NOK Elkjop.no	 Philips HUE LightStrip Plus 1m 209 NOK Elkjop.no	 LIFX Z RGB WiFi Smart LED Light 319 NOK elektroimportoren.no

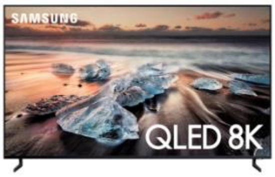
Smart Television	 TCL 55" 4K UHD LED smart-TV 4490 NOK Elkjop.no	 Samsung 55" Q950 8K QLED UHD Smart-TV 39999 NOK Elkjop.no	 Philips 24" Full HD smart LED-TV 3495 NOK Elkjop.no
TV-Stick	 Google Chromecast 349 NOK Elkjop.no	 Amazon Fire TV Stick 539 NOK Powershop.no	 Nvidia Shield TV Streaming Player 2199 NOK Komplett.no

Table 4: List of Smart Devices for the living room

Kitchen			
Device	Example 1	Example 2	Example 3
Smart Fridgecam	 Smarter FridgeCam available 1 799 NOK Elkjop.no		
Fire alarm system	 NEST PROTECT BRANNALARM KABLET 1 299 NOK Power.no	 Xiaomi Mi Fire detector system 300 NOK	 NETATMO SMART SMOKE ALERT 995 NOK Power.no
Smart coffee maker	 Bosch AccentLine CTL636EB6 16 995 NOK Elkjop.no	 MELITTA Barista TS Smart Black Espressomaskin, 9599 NOK whiteaway.no	 Smarter Coffee (2nd Generation) Kaffemaskin 2495 NOK cdon.no
Oven	 Samsung NV7000N, 12 000 NOK Elkjop.no	 Bosch AccentLine serie 8 HNG8764C6 32 995 NOK Elkjop.no	

Smart fridge (+freezer)	 Samsung Family Hub 2.0 44 990 NOK Elkjop.no		
Precision cooker	 Anova vacuum precision cooker 1 699 NOK Elkjop.no		

Table 5: List of Smart Devices for the kitchen

Rest of the House			
Device	Example 1	Example 2	Example 3
Smart-Heating-Thermostat	 Tado Smart AC og varmepumpekontroll V2 1 899 NOK komplett.no	 Netatmo Thermostat V2 1377 NOK komplett.no	
Smart-Door Lock	 ID Lock 150 elektronisk dørlås 3990 NOK Elkjop.no	 Yale Doorman V2N elektronisk dørlås 2990 NOK Elkjop.no	 Aqara S2 Smart C Grade 2418 NOK Baggood.no
Smart Robot Vacuum	 iRobot Roomba i7 støvsuger 10 495 NOK Elkjop.no	 Ecovacs Deebot Slim 2 robotstøvsuger DA5G 1590 NOK Elkjop.no	
Door/window Sensor	 Fibaro System Door/Window Sensor 2 429 NOK futurehome.no		

Motion Sensor	 Philips Hue bevegelsessensor 295 NOK Elkjop.no		
Smart Flood Sensor	 Fibaro water leak detector 487 NOK elektroimportoren.no		

Table 6: List of Smart Devices for the rest of the house

Garden			
Device	Example 1	Example 2	Example 3
Smart outdoor light	 Philips Hue Econic 1195 NOK Komplett.no	 Mipow Garden light 2499 NOK Iphonehuset.no	

Smart door bell	 Ring Door View Cam 1999 NOK Komplett.no	 Nest Hello Video ringeklokke 2749 NOK Komplett.no	
Smart outdoor camera	 Google Nest Cam IQ Outdoor 3699 NOK ClasHolson.no	 Ubiquiti UniFi UVC-G3-AF 1589 NOK ClasHolson.no	 WANSCAM K54 Outdoor 930.03 NOK Banggood.no
Smart water management	 Eve Aqua 995 NOK Elkjpop.no		
Smart weather station	 Netatmo Urban Weather Station 1348 NOK Komplett.no	 Netatmo Rain Gauge 699 NOK Komplett.no	

Table 7: List of Smart Devices for the garden

Bathroom			
Device	Example 1	Example 2	Example 3
Smart toothbrush	 ORAL-B SMART 5 5000 W elektrisk tannbørste 1199 NOK Power.no		
Smart scales	 WITHINGS BODY+ SMART WIFI BADEVEKT SORT 790 NOK Power.no		
Smart vanity .	 The Philips Adore Smart Vanity 2499 NOK Kjell.no		

Table 8: List of Smart Devices for the bathroom

8.3 Risk Assessment

8.3.1 Risk Assessment pilot version

Does the device use a wireless connection to communicate with other smart devices?

Does the device rely on any wireless direct connection to access to internet?

Does it generate/record/collect any private data?

Does it stream or upload data anywhere?

Does the device use secure protocols for authentication and data transmission?

Is the device delivered with a security guide, notes and warnings?

Is the OS based on a known open source kernel?

Is the OS secure and up to date regarding security?

Is it easy to keep updated?

Are the device's settings/data/logs accessible from remote PC/phone/tablet?

8.3.2 First Risk Assessment

Questions

1) Is the device connected with other smart devices?

2) Does the device rely on any wireless direct connection to access to internet?

3) Does it generate/record/collect any private data?

4) Does it stream or upload data anywhere?

5) Does the device use secure protocols for authentication and data transmission?

6) Is the device delivered with a security guide, notes and warnings?

7) Is the OS based on a known open source kernel?

8) Is the OS secure and up to date regarding security?

9) Is it easy to keep updated? (Automatic?)

10) Are the device's settings/data/logs accessible from remote PC/phone/tablet?

Results

List of evaluated Smart Devices			
Family of smart device	**Product**	**Individual grade**	**Final grade**
Smart speaker	Google home mini	4	**4**
	Amazon Alexa	4	
Smart lightbulbs	Geeni Lux	4,5	**3,5**
	Phillips Hue	2,5	
Smart lightstrips	Yeelight LED	3,5	**3**
	Phillips Hue	2,5	
Smart TV	TCL Smart TV	6,5	**6**
	Samsung 8K Smart TV	5,5	
TV-Stick	Google Chromecast	3	**3,5**
	Fire-Tv	4	
Smart fridge	Samsung Family Hub 2.0	4,5	**4,5**
Smart alarm system	NEST Protect Kablet	2	**3**
	Xiaomi Mi Fire detector	4	
Smart oven	Samsung NV7000N	3	**4**
	Bosch Accentline Serie 8	5	
Smart-Heating-Thermostat	Tado Smart AC	5	**5**
	Netatmo Thermostat V2	5	
Robot vacuum	iRobot Roomba i7	5	**4,5**
	Ecovacs Deebot Slim 2	4	
Door/window Sensor	Fibaro System Door/Window Sensor 2	5	**5**
Motion sensor	Philips Hue bevegelsessensor 4	4	**4**
Smart flood sensor	Fibaro water leak detector	5	**5**
Smart outdoor light	Philips Hue Econic	3	**3**
Smart outdoor camera	Ring Door View Cam	5	**5**
Smart water management	Eve Aqua	5	**5**
Smart weather station	Netatmo Urban Weather Station	4	**4**

Table 9: List of evaluated Smart Devices

8.3.3 Final Risk Assessment

Questions

1. Is the device connected with other smart devices?

    1.1 Wired

    1.2 Wi-Fi

    1.3 Is it possible to connect it to 3G, 4G, 4G+, 5G?

    1.4 Are there different connection/communication protocols available on it (Bluetooth, IrDA, Z-Wave, etc)?

    1.5 Does this device control other devices?

2. Does it use a custom network for initial configuration?

3. Is the data transmission over internet in clear text?

4. Does it generate/record/collect any private data?

5. Does it stream or upload data? (Even local-only streaming is dangerous)

6. Is the authentication uncontrolled? (ID/Password in the App is accepted)

    6.1 Does the manufacturer force to change the default password and login? (Answer no is a danger)

7. Does it use multiple factors method for authentication? (Answer no is a danger)

8. Is the OS based on unknown kernel?

9. Does the current version of the OS have known vulnerabilities?

    9.1 Are software upgrades & security patches applied automatically? (Answer no is a danger)

    9.2 Can up-to-date OS versions or release notes easily be found? (Up-to-date means last update or patch was included during the past 9 months.) (Answer no is a danger)

10. Is the device designed to be controlled from a remote network?

11. Are there system logs?

  11.1 Are they stored on cloud?

  11.2 Are they in clear text?

12. Do the manufacturer collect personal data?

  12.1 Does the company claim to follow GDPR's requirements? (Answer no is a danger)

  12.2 Is personal data shared with third parties (even partners)?

13. Are user information and operational data merged?

14. Is the end user licence agreement published? (Answer no is a danger)

  14.1 and if so, does it include security guide or notes & warnings? (Answer no is a danger)

15. Grades:

  15.1 Rate from 1 to 5 the potential impact of a data breach/leak from this device. (1 low impact -> 5 high impact)

15.2 Rate from 1 to 5 the physical impact of a malfunction or a defect of the device. (1 low impact -> 5 high impact)

8.4 Interviews

8.4.1 Visiting Shops

Our team visited Elkjøp shop at Oslo Stortinget in order to collect information about the way smart devices are merchandised. We had a final goal consisting into estimating the degree of knowledge Elkjøp sellers had about the connected devices and their awareness regarding the threads that connected devices bring into our houses. It appears that they have been trained in order to present the advantages of the devices and to explain the benefits for consumers.
We particularly talked about the google home mini, an enhanced speaker that can, when it is paired to other IoT devices, command them forwarding your spoken demands. We tried to discuss the degree of precision of the voice sensors, the risks when this device is paired with for example a smart door lock, the limits of compatibility and to finish, the insurance coverage in case of malfunction and the potential consequences.

Over these topics a seller was interested and informed with knowledge learned from different reviews. This person could come with selling arguments regarding the threads of google home appliance passive listening and the limitation of google home's power over the house. We did not bring the technical talk further to not reveal ourselves.

The major concurrence for this device is Amazon Alexa (not available in Norway). We figured that opinions from a seller to another about which device is better diverge and this because they apparently don't really know the different feature of the other product, so they rely on their appreciation of it. Elkjøp does not give its employees the training to discuss this kind of inquiries. It appears that they have a passive position regarding their customers safety.

Our team also visited a Clas Ohlson shop on the same purpose. We came to similar conclusion because the dialog on a technical point of view was limited. Resellers in Norway are aware of the products available on the market here on the commercial aspect. On the bright side, they always managed to look for information on our behalf whenever we asked questions.

8.4.2 Meeting with Airthings' CTO

Thanks to our coordinator Sinan SOFTIC, we got the opportunity to meet Erlend BOLLE, the CTO of the company Airthings. We had a meeting with him on the 1st October 2019. This was a great opportunity for us to meet a company which is established in the market of smart devices.

Airthings is a Norwegian tech company, founded in 2008, that is led by a team of scientists, engineers and technology professionals. Their goal is to educate people concerning the importance of Radon levels, as well as other air contaminants and develop technology to measure and broadcast information about air pollution. Radon is an invisible gas formed in the Earth's crust. Radon rises and can enter a habitation or workplace through hot water tank, sink, shower, and any microscopic cracks in a building´s foundation.

The company possesses offices in Oslo, Chicago, London, Munich and Quebec with all in all 60 employees.

At first, we got a short informative presentation of the company. Mr. BOLLE introduced the company in general and the different products they have. There are the air quality sensors (Wave, Wave mini, Wave+) deployed just like access points spotted in different places of the house or of the office. Then there is a base unit, the Hub, to control all the access points. Airthings Hub is also a relay as it gathers the data and forwards it to the database. The Hub uses multiple connection ways. Airthings SmartLink protocol is used to communicate with the Access Points. For the internet connection, it is Ethernet and there is also a possibility to plug a sim card.

In a second step, our topic moved to IoT and we had the chance to ask him about risk issues in their company. Airthings is also concerned about cyberthreats. The tech department elaborates scenarios where hackers may intent to corrupt the consumer's database either by populating fake reports of any gas concentration or just by deleting needed information.

The communication from the hub to the cloud is secured with strong mechanism of hash, encryptions and asynchronous key exchange. Therefore, the domain of risk they focus on is between the access points and the hub. As the access points are paired to the base units, they imagined a situation where the hacker fakes an access point to pair his custom device to the controller. By performing this process, the hacker may push wrong information and/or malicious codes in order to corrupt the consumer's database.

They overcame this risk with a simple update on the latest generation of their products. To pair a device with the controller, you need a serial number which matches and a unique ID number that goes with it. Therefore, there is no possibility for a counterfeit device to be paired with the Hub.

Finally, Mr. BOLLE had a look on the second version of the risk assessment, we created and passed one of their major products through this evaluation system

Questions	Answers
1) Is the device connected with other smart devices? 1.1> Is it possible to connect it to 3G, 4G, 4G+, 5G? 1.2> Are there different connection / communication protocols available on the device (Bluetooth, IrDA, Z-Wave, etc) 1.3> Does this device control other devices?	1) Yes 1.1 Yes (2G) 1.2 Yes (Bluetooth) 1.3 Yes (through the cloud)
2) Does it use a custom network for initial configuration?	2) No
3) Is the data transmission over internet encrypted?	3) Yes
4) Does it generate/record/collect any private data?	4) Yes
5) Does it stream or upload data? (Even local network streaming is dangerous)	5) Yes
6) Is the authentication controlled? (Code to get in the app maybe) 6.1> Does the manufacturer force to change the default password and login?	6) Yes 6.1 Yes
7) Does it use multiple factors method for authentication?	7) No (Not sure)
8) Is the OS based on a known open source kernel?	8) Yes
9) Is the current version of the OS secure? 9.1> Are software upgrades and security patches applied automatically? 9.2> Can we easily find up-to-date OS versions or release notes?	9) Yes (Hard to answer, it is not sure) 9.1 Yes 9.2 No
10) Is it possible to control the device from a remote network?	10)Yes
11) Are there logging information?	11) Yes
12) Do the manufacturer collect personal data?	12) Yes
13) Is personal data shared with a third party (even partners)?	13) No
14) Are security guide or notes & warnings available anywhere?	14) No
15.1) Rate from 1 to 5 the potential impact of a data leak from this device. (1 no risk -> 5 risky)	15.1) 1- 2
15.2) Rate from 1 to 5 the physical impact of a malfunction or a hack of the device. (1 no risk -> 5 risky)	15.2) 3-4

Table 10: Results of Risk Assessment of a product from Airthings

After the assessment, we discussed the relevance of the questions we went through. It was a very interesting exchange and Mr. BOLLE suggested to us to analyse the way data is saved whether on the cloud or on the device. If user information and operational data are separated, it proves a concern for the manufacturer to protect its consumers.

In conclusion, this interview was a very constructive add-on to our project.

This meeting was extremely helpful. We had a first insight of a Norwegian company, an unique opportunity for us, foreign students.

Airthings is still a small company, but it operates at world scale and is growing. Their concern about cybersecurity is real and underlines the importance of the threats related to smart devices. Knowing that companies like this, which are designing the next generation smart devices, care so much about cyber threats shows the importance of our project as RELINK team is investigating the same threats from a consumer point of view.

Figure 9: Picture of Group M with Erlend Bolle (CTO, Airthings)

8.4.3 Meeting with experts

Thanks to our supervisors Terje and Anthony we had the opportunity to meet Hedda Marie, a computer science (programming, data bases, security engineering) student. In parallel of her courses, she will start teaching cybersecurity and hacking in December for students who are curious about those fields. Students will learn the hacking part from ground zero knowing most of them have computing sciences background. The first achievement will be the basic learning (what is hacking etc). She will teach her students that hacking is forbidden. When it comes to hacking websites, it goes very fast for example SQL injection is a language that can be learned in only 10 minutes.

After Hedda's global presentation, we moved the topic to smart devices. We asked her if she had smart devices at home. She did not have any except a smartphone, but she might be interested into having some in the future. Therefore, we took an example of a smart laundry machine. She could buy it, but she would be scared about the private data that may leak out of her home. Then, we talked about which criteria makes her choose her smartphone. For her, the main criteria are the price, the convenience, the open source system like Android or IOS.

Then, we talked about the risk assessment. She would be interested in using it only if it is not expensive, before purchasing the smart devices. The vision that she had, was an assessment app, not a physical one. Next, we presented her the risk assessment, to have another point of view of someone who is in the same field. First, we explained her each question and she suggested us some modifications. When it comes to private data, she mentioned that in Norway it was possible to request our personal data. Moreover, she gave us a website, datatilsynet.no, which provides all the rules and the laws about privacy.

In her point of view, the devices which are the most discreet are usually less protected. Devices having multi-protocols connection are also potentially more dangerous. She gave us an example with a doll which has a smart device inside it. As the user maybe will only setup the Wi-Fi settings, if Bluetooth is enabled with its default configuration, someone can just exploit the Bluetooth connection to access the system core data and control the doll.

To finish, we asked her what the scariest smart device is on the market. She thought about kid toys, because they can be moved around and it is not usually secured, everything is in clear text. They are possibly weak points in network, even if Bluetooth is about ten meters, toys with cameras could take pictures of kids. In her opinion, cheap devices have cheap securities.

In conclusion, we want to thank Hedda for her time and the quality of her expertise. It was very interesting to discuss with her and what she said will be very helpful for the next step. We wish everything will be fine for her, with her future class and that she will provide all the knowledge to them.