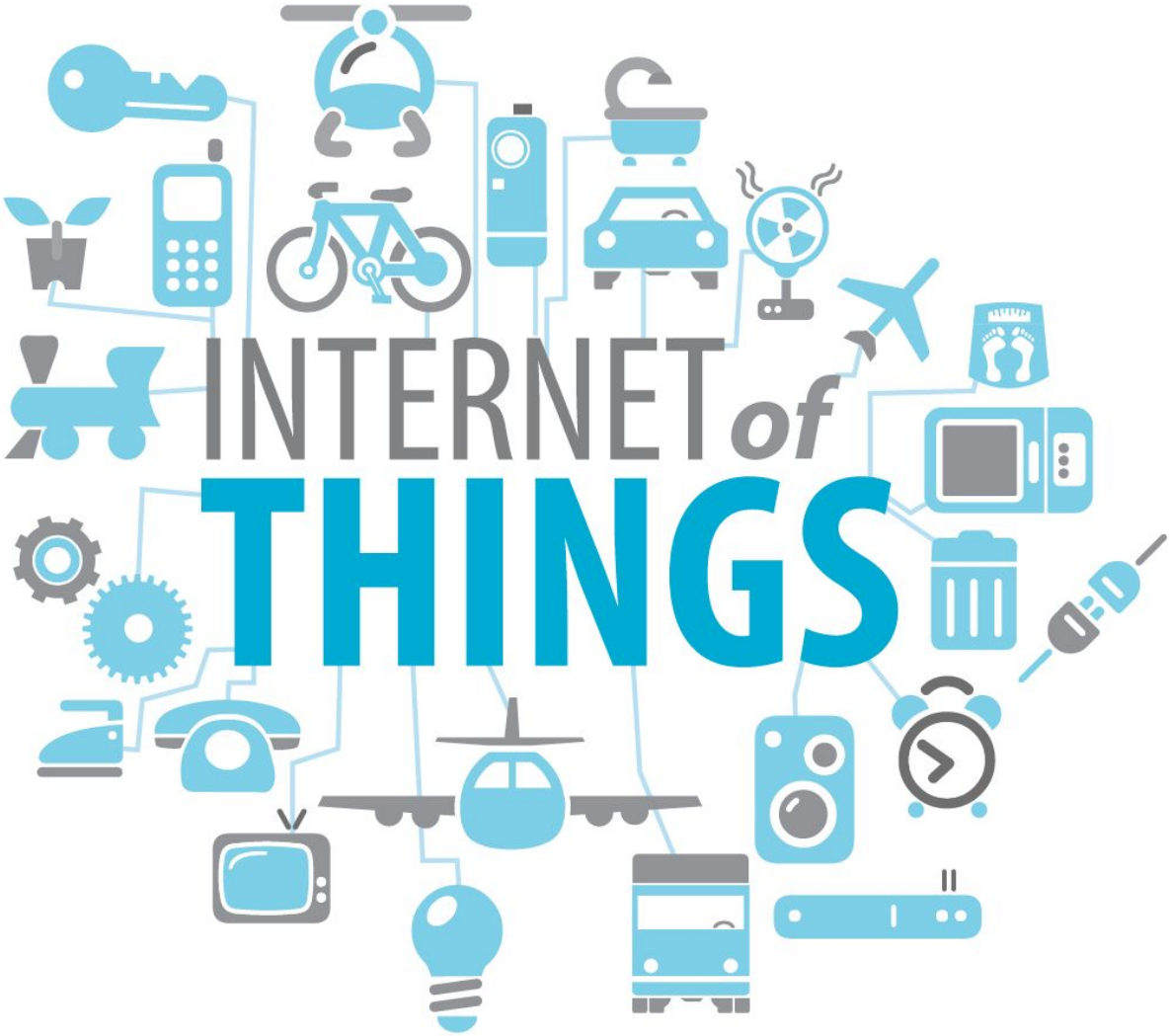
Intersect Research Plan

General guidelines for IoT devices and applications



Merlijn Vermeer, Marc van Bommel, Rick Theeuwes, Thomas van Heel, Joel Adams, Anouk Brondijk, Hristo Slavchev

09.16.2020
Version: 1.0

Version History

Version	Date	Changes	Author
0.5	16-09-2020	Initial setup and styling.	Merlijn Vermeer
1.0	17-09-2020	Finalizing the first version of the document	Group
1.1	24-09-2020	Improving document with feedback	Group

Approval

Version	Date Approved	Name	Function	Signature
1.0	16-09-2020	The group	none	-

Distribution

Version	Date send	To/where	Reason
1.0	25-09-2020	Canvas	Feedback
1.1	24-09-2020	Canvas	Feedback

Table of contents

1 Introduction

This document describes the research conducted on behalf of the INTERSECT project. The goal of this project is to write general guidelines for securing all IoT devices and applications. We will research more on a given smart office and smart industrie case but we will write the guidelines more in general but based on the specific research we did. INTERSECT is research for NWO about securing all IoT devices and applications so the goal of INTERSECT is to *drive the change to a safe and secure IoT environment for the digital transformation in the Netherlands(INTERSECT, 2019).* Our part in this vision will be researching vulnerabilities in existing projects and writing guidelines based on our findings.

This document will describe our plan of tackling the research needed for this project. Starting with a description of our project and the Stakeholders, then we have research questions, planning, a summary of the organization and Stakeholders, and quality control.

2 Project

2.1 Description

The project is to create a general guideline for IoT applications and devices in general. There are generalized guidelines out there, but this project aims to create one that is accessible and easy to read to both consumers and engineers. In the end, all the guidelines and additional information should be on a website, where anyone may view this.

2.2 Scope

The Scope of this project includes 4 major sectors, Smart industry, Smart Health, Smart Mobility and Smart Cities. We will limit the research to these four sectors and their IOT devices. All other IOT sectors will be excluded.

2.3 Research question

The main research question is: *What are the most common vulnerabilities in IoT devices and applications and what guidelines should be followed to improve general IoT security?*

In order to create the guideline, we must first determine what vulnerabilities there are in IoT devices and environments. We will take a look at hardware testing, but this will not have the main priority instead of pentesting over the network. We do this by researching two IoT applications we've been given by the stakeholders. The first is for the air scrubber, which is an industrial machine that sucks out dirtied air, cleanses it, and blows it back in. The second is for Smart Office, a system that measures the Co2 and noise levels in the air and gives suggestions to improve productivity. Next to the applications, we will find information on the internet and maybe ask questions to people who have experience in fields like this.

Once we've found the information we need, we'll make the guideline itself. This guideline will contain the vulnerabilities we've found in the applications and with online information. This will answer the question as well, as once we have the guideline we will be able to improve general IoT device security.

2.4 Results

The result of this project should be a clear document with guidelines on how to secure an Iot device or environment. The guidelines will be general for all IoT devices, to be used by owners, manufacturers and end-users of IoT.

3 Key Success Factors

3.1 Schedule

Every Wednesday and Thursday will be assigned to work on the project.

3.2 Cost

There are no costs to this project.

3.3 Stakeholder satisfaction

It is important that the stakeholder is satisfied with our project. To assure the project is not running into any problems, the business case will be aligned with the development team.

3.4 Alignment to business case

It is important to align the business case with the team working on the project.1

4 Research approach

What are the most common vulnerabilities in IoT devices and what guidelines should be followed to improve general IoT device security?

What is IoT?

This project is purely focussed on IoT devices, so it is required to have some knowledge of IoT before we can secure these devices.

Library: Literature study

Library: Available product analysis

Library: Community research

What are the most commonly found vulnerabilities in IoT devices and environments?

Our guidelines need to be as generic as possible in order to work for as many IoT devices as possible, so the most common vulnerabilities need to be known to make clear guidelines.

Field: Document analysis

Library: Literature study

Field: Problem analysis

What vulnerabilities can be found in the Air-Scrubber and SmartOffice projects?

The Air-Scrubber and SmartOffice are part of our project, we will partially base our guidelines on the results of the vulnerability assessment of these two projects.

Lab: Security test

Workshop: Code review

Showroom: Ethical check

What design patterns must be followed in order to prevent common vulnerabilities?

We will look into design patterns that could improve the vulnerability of IoT devices. These patterns can be coding design patterns but also infrastructural, like fixes for the OS system that runs the application. We will implement these best practices in the IoT project we will be testing out and try out if these design patterns are really securing the IoT device.

Library: Best good and bad practices

Workshop: Prototyping

Library: Design pattern research

What are the good guidelines and best practices that IoT devices should follow to prevent vulnerabilities?

There are already many companies that made guidelines for IoT devices. Our goal is to combine all those guidelines and make additional changes of maybe things that changed over the time since the document was made. When searching for those guidelines and best practices we will be trying those out and checking if these guidelines can completely secure an IoT device.

Library: Literature study

Field: Problem analysis

Library: Best good and bad practices

Workshop: Prototyping

Showroom: Product review

5 Planning

Sprint 1: school week 1-4, normal week 36-39

31 august - 25 september

Defining the scope and searching IoT devices

Setting up testing environments

Gathering extra applications/devices for testing

Gather and discuss security requirements

Discuss BlackBox Whitebox

Define security threats for the system to develop and perform a risk analysis.

On 11 September the individual ethics analysis and the individual research approach need to be handed in.

On 18 September the preliminary research should be handed in.

On 25 September the research plan needs to be handed in.

Sprint 2: school week 5-8, normal week 40-43

28 september - 30 october

Red teaming and security research

Researching possible known security flaws

put the threats in a secure design through misuse cases.

There will be a week of vacation from october 19 until october 23.

On 30 October we need to hand in all sprint 2 products, reviews, and reflection.

Sprint 3: school week 9-12, normal week 44-47

2 november - 27 november

Executing the penetration tests(Research flaws)

Work out security controls to limit the threats in your misuse cases

Implement the security controls

Implementing security measures

On November 27 we need to hand in all sprint 3 products, reviews, and reflection.

Sprint 4: school week 13-16, normal week 48-51

30 november - 8 january

Gather all information and create an advice report.

Testing the fixed security flaws

Test the security controls by developing test cases for the threats. Add fuzzing tests.

There will be two weeks of vacation from december 21 until january 3rd.

On 8 Jan we need to hand in all sprint 4 products, reviews, and reflection.

On 15 Jan we need to hand in all final products, reviews, and reflection.

On 29 Jan we need to hand in the ICT in practice products for the ICT symposium.

1.1. Project organization

Communication	Purpose	Medium	Frequency	Audience
Project team meeting	Review the status of the project	Online	Weekly	Project team
Stakeholders meeting	Review the status of the project	Online	Every 4 weeks	Project team, Product owner, Stakeholders
Casper meeting	Review the status of the project	Online	Weekly	Project team, Product owner

1.2. Scrum

Our scrum sprints are four weeks long, everyday we have a standup at 9 o'clock. In this stand up we talk about the day before and the planning for the day.

The backlog contains all the stories for our project. These stories are divided into subtasks. All the stories are also connected to an epic. The entire backlog can be found in appendix B.

For something to be done according to our definition of done it needs to be checked by another student for any mistakes. All our code should be tested and documented. If the document or code contains any errors or mistakes it should be put back to active on our scrum board and rechecked after the problems have been fixed. The definition of done can be found in appendix C.

6 Quality

To assure the quality of our work we will be reviewing and testing everything we do. Our scrum board will include a column called reviewing to assure every ticket will get reviewed.

1.3. Reviewing

- We will review what we have done at the end of each week, during our group meetings.
- All the documents will be reviewed using google docs and everyone will be able to access and update them or comment on things that should be changed
- There will be code reviews during the implementation phase. These code reviews will be done on GitLab by using merge requests. Another member of the group needs to review the written code and make feedback if there is anything wrong with it.
- Every ending of the sprint we have a meeting with our stakeholders, for the review of all our new documents.
- During this meeting, new requirements will also be documented.

1.4. Testing

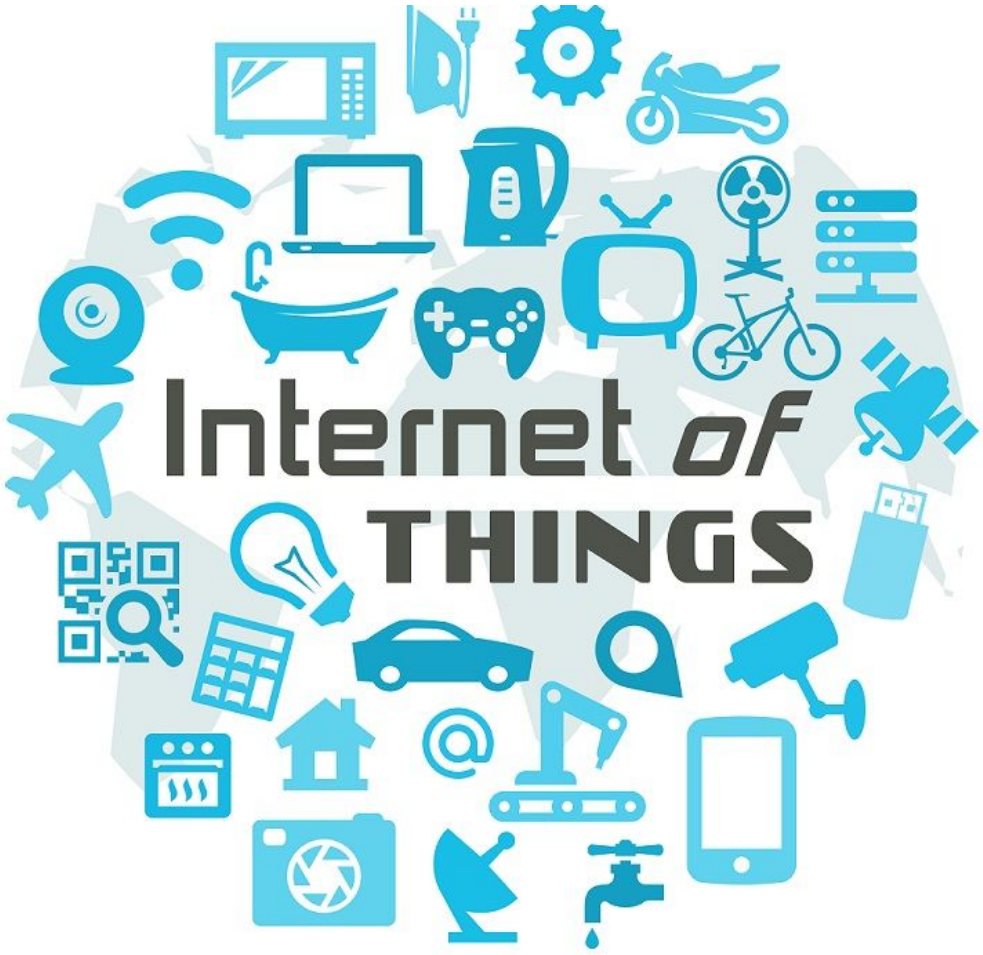
- Unit testing will be made on the code to ensure that everything works if we change things up.
- Manual testing will be used to test important pieces or things that cannot be automated
- Pentesting is used to test if the security measures work.

7 Bibliography

- *INTERSECT*. (2019, 1 november). INTERSECT. https://www.nwo.nl/onderzoek-en-resultaten/onderzoeksprojecten/i/00/33700.html

Appendix A: Preliminary research

Initiation Phase



Merlijn Vermeer, Anouk Brondijk, Joël Adams, Hristo Slavchev, Marc van Bommel, Rick Theeuwes, Thomas van Heel

24/09/2020

Introduction

In this document, we will describe the initiation phase. The main goal of this project is to find the most common vulnerabilities that are reported in such devices. The IoT devices that we are going to research and secure are Industrial and Home/Office IoT devices. The research phase is of great importance for the success of such a project and this is why our main focus at the beginning of this project will be to define the scope of the project.

The stakeholders of this project are Teade Punter and Mark Metsen. We are a group of seven students and we are making sure that the division of the work is separated equally, considering the strengths and the abilities of everyone. This project will help us develop and improve our knowledge of cybersecurity and to learn more about IoT devices and their security.

In the first chapter, we talk about the wishes of the clients and stakeholders. In the second chapter, we'll talk about the current situation, what's already there and what isn't. In the third chapter, we'll talk about how we will develop the guidelines and what test environments we will use for lab research.

In the fourth chapter, we will talk about which technologies we will be using. After that, we'll talk about the requirements and functionality of the guidelines, and which user groups will be using them. Lastly, there will be a few apendices: interview reports, risk- and threat analysis, and the privacy impact assessment.

1 Client and stakeholder wishes

In general, the client wants to have security guidelines of the most common flaws of IoT devices. The client demands that the new documentation that will be used to secure their devices needs to be clear and easy to read. This is, because it will be applied to real life situations. The guidelines have to cover the most used IoT devices, because of their broad range of use and therefore their great potential for critical exploits. It is expected that the most commonly found exploits will be covered and that section specific exploits will be named and/or highlighted for the users own research.

2 Current situation

Currently, there are several kinds of guidelines present. There are guidelines from OWASP, who put together a top ten of most common vulnerabilities and how to fix them. Enisa, European Union agency for Cybersecurity, goes a lot more in-depth with their Good Practices tool. (*ENISA Good practices for IoT and Smart Infrastructures Tool*, z.d.) With that tool, you can filter by security domain, security measure and threat group. Each entry is succinct but clear and has a whole list of sources present. Enisa also has articles about current events, such as how to set up securely at home in these times of Corona.

Intersect's project, An Internet of Secure Things *(An Internet of Secure Things - INTERSECT, 2019)*, aims to go a bit deeper and a bit more specific, while still keeping the scope as broad as possible. We haven't received information about the current state of their project.(*OWASP Top 10 IoT*, z.d.)

3 Development and test environment

For each project we are going to test, we need a separate Testing environment. Right now this means that we need a testing environment for the Air Scrubber project and one for the Smart office project. Both test environments should have a server running the program and a server running the sensor mock to provide data.

The Development environment is only needed if we are going to improve the security for one or both projects. which is not the main goal of this project. However if we decide to improve a project we need a continuous integration environment, which automatically tests and deploys to our server. This environment should also update the version running on the test environment in order to pentest the improved security measures.

4 Technology

The git of the projects we got from Taede Punter.
Here we found the following technologies.

The Technology that is found in the 2 projects (smart office and air scrubber) are:

- Air Scrubber application written in java
- Smart Office application written in C#
- Sensor code written in C / Arduino code

For both projects there are scanners and sensors used to measure real life values, the ones already known are:

- Scanners for air quality for Air scrubber.
- Sound sensor for Smart office.
- Ammonia sensor for Smart office.

5 Description

We will describe all our user groups and requirements for our project.

User groups

Manufacturers, developers end-users and owners of IoT devices and software.

Functionalities / use cases

The guideline’s function is to prevent common vulnerabilities in IoT devices.

Security threats and risks

If our guideline document has mistakes in it, it could have an impact on the security of IoT devices, since developers and manufactures followed our guidelines.

Misuse cases

The guidelines can be used by a hacker to identify vulnerabilities in existing IoT devices, which can be exploited.

Non-functional requirements

The guidelines should be easily accessible for everyone.
The security aspects will be taken into account.
The guidelines should be easy to read.
The guidelines should be written in English, to be available to a wider audience.
We are going to take into account the response time of the website with the guidelines.

Privacy

Because the end product is a set of guidelines, there will be no user data collected.. This means there is no privacy risk.

Ethical aspects

It should be made clear that the guidelines are only guidelines not hard rules to follow. They should not be used to exploit devices without the owner's permission. Further, it should be made clear that there could always be errors and mistakes present in the guidelines.

Usability

The guidelines can be used to improve the security of your IoT device(s). It is not for illegal usages.

Performance

Because this project is not a product or site itself there are no real performance requirements. If the guidelines are easily followed and read, its performance is satisfactory.

Maintainability

The guidelines can be maintained by updating if new security flaws are discovered. The guidelines will be public (such as github pages) so everyone can see them.

6 List of sources

- *OWASP Top 10 IoT*. (z.d.). https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf Geraadpleegd 16 september 2000, van https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf
- *An Internet of Secure Things - INTERSECT*. (2019, 1 november). NWO.nl. https://www.nwo.nl/onderzoek-en-resultaten/onderzoeksprojecten/i/00/33700.html
- *ENISA Good practices for IoT and Smart Infrastructures Tool*. (z.d.). enisa.europa.eu. Geraadpleegd 24 september 2020, van https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool

7 Appendices

Interview reports

02-09-2020 we did an interview with all the stakeholders(Taede Punter, Mark Madsen, Ron Mélotte and Casper Schellekens.) We have discussed all the questions that we had, such as:

- What is the project (scope)?
- Do we get the source-code, or is it black-box?
- Do we do physical tests, or are they completely over network?

So the status is not vague anymore, because we have all the answers we needed. With this information we could start the research and the corresponding documentation. We asked for the permissions of the source code of both projects.

09-09-2020 Casper Schellekens: We have discussed the individual research approach and the ethical analysis. We decided to have regular meetings every Wednesday at 11:00.
We discussed what should be in the scope and what not. We received the source code of the Airscrubber and Smart home.

16-09-2020 Casper Schellekens: We have discussed the scope, the phase 1 document and the research plan. Our guidelines should be as generic as possible. We discussed the ability and the advantages of being present at the Intersect conference on Cyber Security of Internet-of-Things. So everyone registered for this webinar, we all think it will be useful. There is still no proper communication with CTouch. Casper will call them this day and try to get in contact that way.
We will be working on our phase 1 document and after that is done the research plan that will be due the week after that.

Risk analysis

Threat	Impact description	Impact level	Proba-bility	Level security controls	Controls[1]
DDoS	Downtime, Reputation damage, The resources will be unavailable	High	Low	Standard Control Set and Incident Response procedures needed	Configure the network hardware against DDoS attacks.Protect the DNS servers. Web Application Firewall
Script Kiddies, opportunists	Stolen data	Medium	Medium	Moderate Level of security needed	Backups are made regularly. Input is being filtered.
Malware infection	Critical data could be lost	High	Medium	High Level set of security needed	Antivirus installed, regular updates
Phishing	Divulging confidential information, downloading malware	High	High	Very High Level of security necessary	Spam filters, secure mail- and dns servers, employee training
Data breach personal data	Financial damage, Reputation damage, Claims, Fines	Very High	Medium	Very High level of security necessary	Check passwords for strength, check code for hard coded passwords, input filtering, two factor authentication
Stealing Confidential business data	Financial damage, Claims, Reputation damage	High	Low	Standard Control Set and Incident Response procedures needed	Good firewall rules, safe company policies, input filtering, two factor authentication
hacktivists	Financial damage, The resources will be unavailable	Medium	Low	Standard Control Set and Incident Response procedures needed	Secure backup for main services. Setup good firewall rules for blocking traffic.
state actors	Environmental damage/safety, Human safety, Physical damage	Very high	Low	Standard Control Set and Incident Response procedures needed	Secure backup for main services. Setup good firewall rules for blocking traffic. input filtering, two factor authentication

[1] Overall is patching an important part, to reduce the options for hackers

Threat analysis

Based on some workshops we got and the research we did we made some threat analysis for all the industries.

smart energy:

Threat Actor	**Motivation**	**Methods**
Script kiddies	Thrill	DDoS tools, Metasploit
Cyber espionage	Intellectual property	SQL-injection, XSS, exploits, CSRF, privilege escalation
Cyber warfare	Cripple the energy network of a country	SQL-injection, XSS, exploits, CSRF, privilege escalation

smart industry:

Threat Actor	**Motivation**	**Methods**
Script kiddies	Thrill	DDoS tools, Metasploit
Hacktivists	Protest	SQL-injection, XSS, exploits, CSRF, privilege escalation
Cyber espionage	Intellectual property	SQL-injection, XSS, exploits, CSRF, privilege escalation
Cyber warfare	Cripple the industry of a country	SQL-injection, XSS, exploits, CSRF, privilege escalation

smart health:

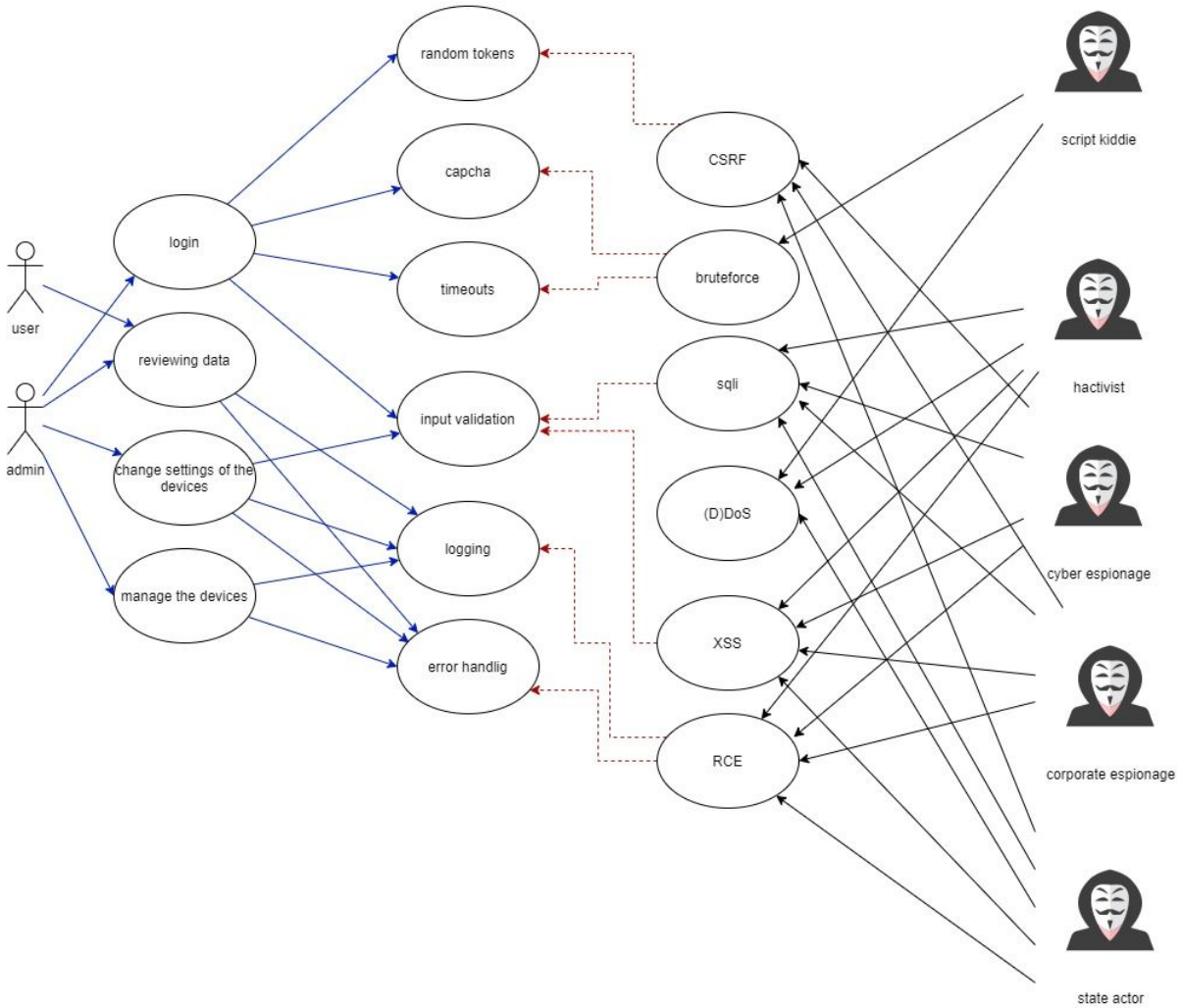
Threat Actor	**Motivation**	**Methods**
Cyber espionage	Intellectual property	SQL-injection, XSS, exploits, CSRF, privilege escalation
Cyber warfare	Cripple the healthcare of a country	SQL-injection, XSS, exploits, CSRF, privilege escalation

smart mobility:

Threat Actor	**Motivation**	**Methods**
Cyber espionage	Intellectual property	SQL-injection, XSS, exploits, CSRF, privilege escalation
Cyber warfare	Cripple the infrastructure of a country	SQL-injection, XSS, exploits, CSRF, privilege escalation

Misuse diagram

We made a general misuse diagram that takes all attack vectors in account from every IoT device industry. These are worked out in misuse cases below.



Misuse cases

We have worked out multiple misuse cases from all the attack vectors.
These are all based on general IoT devices and the possible attack vectors.

Name	**UC1**: SQL injection
Summary	Due to a lack of filtering a user can enter SQL code and that gets executed
Description	1. The actor enters SQL-code in a textbox 2. The SQL-Server executes the code 3. The actor receives the result (depending on the injected function) 4. the actor can read and adjust the entire database
Security	1. Separation of data 2. Roles 3. Input filtration
Assumptions	-
Worse case threat	The actor can read, adjust and delete all data in the database.
Prevention	b1. The actor can see and adjust a part of the data but not everything. b2. The actor can see or adjust data b3. The actor can not do anything
Stakeholders and threats	The stakeholders are all the users of the IOT device, because all data from the device(s) connected to the database can be leaked.
Scope	All data saved in the database.
Solving	

Name	**UC2**: XSS
Summary	Due to a lack of filtering a user can enter JS code and that gets executed
Description	1. The actor enters JS-code in a textbox 2. The client executes this code on another user 3. The actor can possibly steal cookies, alter the page and or follow the user on the page.
Security	1. Input validation
Assumptions	-
Worse case threat	The actor can execute all JS-code
Prevention	b1. The actor can not enter JS-code
Stakeholders and threats	The stakeholders are all users. It is difficult to figure out if someone is using XSS.
Scope	All pages of the IOT admin environment.
Solving	

Name	**UC3**: Account takeover
Summary	By abusing an exploit the actor can get access to the account of another user.
Description	1. The actor abuses an exploit to gain access to a login-token or a name password combination. 2. The actor uses this data to login.
Security	1. 2 factor authentication at logging in. 2. Give users only the necessary rights.
Assumptions	- There is an exploit in the system that allows the actor to gain someone's info.
Worse case threat	The actor has full control of the compromised account and is able to steal data and inflict damage, based on the given rights of the account.
Prevention	b1. The actor can do nothing with a username and password. b2. The actor can only do things the account has access to.
Stakeholders and threats	The stakeholder is the user of whom the access information is stolen. De damage depends on the rights of the user.
Scope	The compromised user.
Solving	

Name	**UC4**: (D)DoS
Summary	By executing multiple requests or by a (D)DoS error in the application an actor can shutdown the system.
Description	1. The actor has a bot-net online or found a (D)DoS-error in the application 2. the actor activates the attack
Security	1. using a (D)DoS-blocker 2. adding firewall rules to prevent certain (D)DoS attacks.
Assumptions	-
Worse case threat	The entire system is down and unavailable.
Prevention	b1. A (D)DoS is no longer possible, however a dos error is still possible. b2. Certain (D)DoS attacks can be prevented but not all.
Stakeholders and threats	No one can use the IOT device during the attack.
Scope	The IOT device.
Solving	-

Name	**UC3**: CSRF
Summary	By abusing an authentication cookie a actor can make a request from another site to the IOT device
Description	1. The actor makes a request from another site with an authentication cookie from the IOT device to the authenticated environment. 2. The web server executes the request thinking it is coming from the actual authenticated user.
Security	1. Random tokens 2. Short lifespans for the tokens.
Assumptions	
Worse case threat	The actor can execute things on behalf of the user of the IOT devices.
Prevention	b1. CSRF Token b2. The actor has only a small period of time to use the token. Meaning the actor most likely has an outdated cookie.
Stakeholders and threats	The stakeholder is the user of whom the authentication cookie is stolen. De damage depends on the rights of the user.
Scope	The compromised user.
Solving	-

Name	**UC4**: RCE
Summary	By injecting code or uploading a file the actor can run arbitrary code on the system
Description	1. The actor injects code or uploads a file to the target. 2. The actor executes this code and gets full control of the system
Security	1. Restricting the rights of the system-users 2. Validating all user input. 3. Preventing arbitrary file upload
Assumptions	
Worse case threat	The actor has full control of the compromised system, as far as the system rights let him
Prevention	b1. Input validation b2. Certain (D)DoS attacks can be prevented but not all.
Stakeholders and threats	The actor has full control of the device, every user is a stakeholder.
Scope	The entire IoT device.
Solving	

Privacy Impact Assessment

Almost all IoT devices are connected to a personnel, office or industrial network. The compromise of these devices could mean that an attacker can get access into the private network, allowing them to scan other devices and gain information from the network.
The devices can also be used to monitor the behavior of the end-user. This information can be gathered by the manufacturer, the owner and a criminal to be used for various reasons, mostly without the user's consent. No data of the end-user should be made public, this means that all communication must be over secured channels and all saved data must be protected. The manufacturer can save user data, but they should be capable of securing the data and have full explicit permission on keeping it. If the manufacturer wants to use the data for any purposes whatsoever, they also need explicit permission of the end-user, assuming that the usage of the data is allowed.
The GDPR is very broad on what is to be treated as personal data, so it is best to just assume that all data collected is personal data and should not be collected or stored without the permission of the end-user.

Source:
https://gdpr-info.eu/chapter-3/

Appendix B: Product backlog

IN Sprint 1 11 issues

Sprint plannen

initiation of the project
17/sep/20 10:23 AM • 25/sep/20 10:23 AM

IOT onderzoek	~~IN-1~~	-
IOT guidelines onderzoek document opstellen	~~IN-2~~	-
IOT onderzoek document items categoriseren	~~IN-3~~	-
Defineer Scope in documentatie	~~IN-5~~	-
Searching IOT devices	~~IN-7~~	-
Discuss blackbox whitebox	IN-8	-
Gathering extra applications/devices for testing	IN-9	-
Gather and discuss security requirements	IN-10	-
Opzetten testing omgeving	IN-4	-
Initiation phase document	IN-11	-
Research plan document	IN-12	-

IN Sprint 2 6 issues

Sprint starten | Sprint plannen

Security research (flaws)	Research	IN-13	-
Security Research document	Documentation	IN-22	-
Pentesten test omgeving	Testing	IN-23	-
Opstellen pentest rapport (per device)	Documentation	IN-24	-
put the threats in a secure design through misuse cases	Testing	IN-15	-
Hand in your products, reviews and reflections	Feedback	IN-26	-

IN Sprint 3 5 issues

Plan sprint

Executing the penetration tests(Research flaws)	Testing	IN-18	-
Work out security controls to limit the threats in your misuse cases	Implement	IN-19	-
Implement the security controls	Implement	IN-20	-
Implementing security measures	Implement	IN-21	-
Hand in your products, reviews and reflections	Feedback	IN-27	-

IN Sprint 4 5 issues

Sprint plannen

Create advice rapport	Documentation	IN-25	-
Test the implemented solutions	Testing	IN-28	-
Develop test cases for the threads of the security controls	Documentation	IN-29	-
Fuzzing tests for the security controls	Testing	IN-30	-
Hand in your products, reviews and reflections	Feedback	IN-31	-

Definition of Done

User stories

Once a Jira ticket is done, the outcome must be looked at by one other person. Any document will be looked over and spell checked or corrected, and any code must be commented and may have unit tests passed. Any pentest must be looked over to see if something was missed or went wrong and if the report is correct. If the document or code needs to be fixed or changed, the story will go back into active state, and once these changes are through it will be looked over again.

Epics

Epics,(complete documents, pentests, and code proof of concepts) will be defined as done once it's looked over by one person. Any document will be looked over and spell checked or corrected, and any code must be commented and may have unit tests passed. Any pentest must be looked over to see if something was missed or went wrong. If anything needs to be changed or fixed, a new ticket will be made and put in the current sprint. This user story ticket will be judged by the above criteria. Once that ticket is done, the epic will be judged again.

Release

Once we have full documents or a full proof of concept, or any other product, two people will look over this. The release is done once all the epics and user stories pertaining to this product are done; everything compiled and present, the product is complete, everything is spell checked and checked for mistakes, and code is commented and passes the tests. We may also ask the teachers for their feedback. If anything is missing or wrong, a new user story will be made to fix it.

Sprint

A sprint will be defined as done once all user stories are done and reviewed by at least two other people. At the end of each sprint, there will be a retrospective to talk about the sprint and what has gone right and/or wrong. Any user stories that aren't done will be carried over to the next sprint.