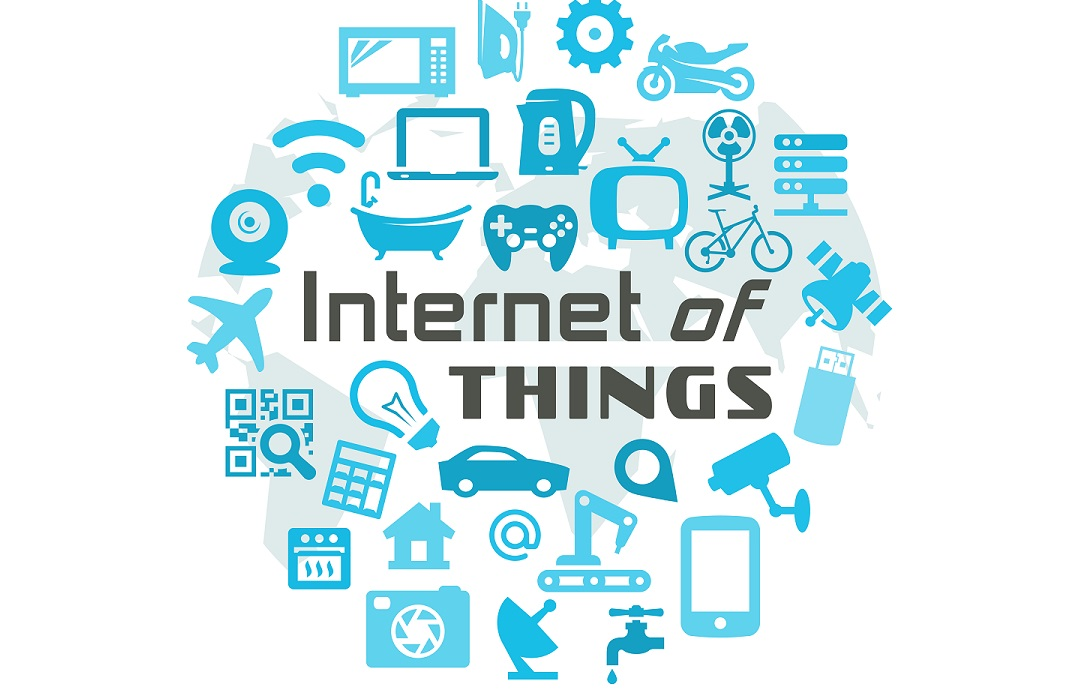
Initiation Phase



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

*24/09/2020*

# 

[**Introduction**](#_g0tlqpbtdgz8) **3**

[**1 Client and stakeholder wishes**](#_8sk4lwtvsdl) **4**

[**2 Current situation**](#_folart45n5i3) **4**

[**3 Development and test environment**](#_ojhby9h4kymd) **4**

[**4 Technology**](#_276qe7a6s4vh) **5**

[**5 Description**](#_oigi94sxdgq9) **5**

[User groups](#_n4lx3q6kywgd) 5

[Functionalities / use cases](#_j6lww83k12yd) 5

[Security threats and risks](#_1mpy9d4kjf9k) 5

[Misuse cases](#_rwbg2u40yekg) 5

[Non-functional requirements](#_131a86yasdhc) 5

[Privacy](#_4vzt8fkrjts7) 6

[Ethical aspects](#_3sa0mft9tnxe) 6

[Usability](#_hloa8vaozzeq) 6

[Performance](#_wdu9zz14c0t6) 6

[Maintainability](#_tgw4ggpb7tb0) 6

[**6 List of sources**](#_kpzawd8bkzlf) **7**

[**7 Appendices**](#_qzln5s4vrwd1) **7**

[Interview reports](#_64r7q2sp0ogs) 7

[Risk analysis](#_ie3508jhwyw8) 8

[Threat analysis](#_xdf3iojqs1k5) 9

[Privacy Impact Assessment](#_6fv24w9fz49t) 14

# 

# 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.

## 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** | **Probability** | **Level security controls** | **Controls[[1]](#footnote-0)** |
| 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 |

## 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:*

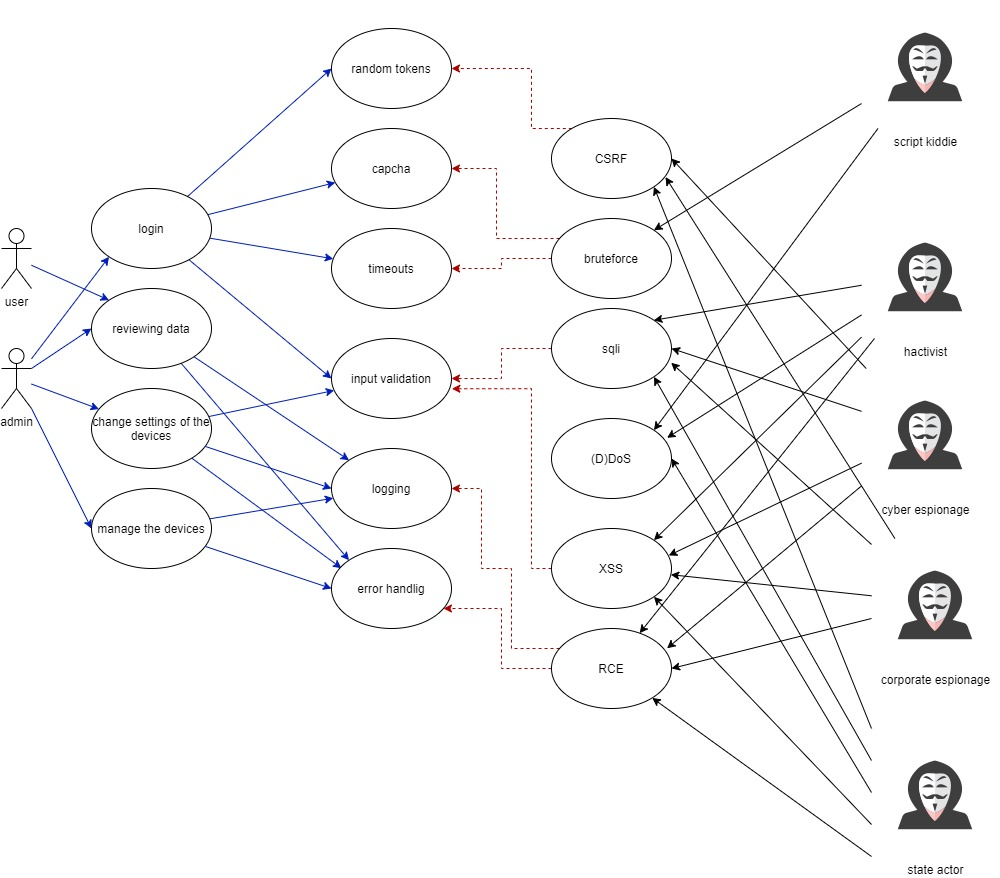
|  |  |  |
| --- | --- | --- |
| **Threat Actor** | **Motivation** | **Methods** |
| Cyber espionage | Intellectual property | SQL-injection, XSS, exploits, CSRF, privilege escalation |
| Cyber warfare | Cripple the healthcare of a country | SQL-injection, XSS, exploits, CSRF, privilege escalation |

*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/>

1. Overall is patching an important part, to reduce the options for hackers [↑](#footnote-ref-0)