|  |  |
| --- | --- |
| **Faculteit Industriële Ingenieurswetenschappen** |  |

Certificatieprogramma Beveiliging IoT

Datum: 15/12/2018

Auteur: Wouter Falise

Interne Promotor: Prof. dr. ir. Nele Mentens

Externe Promotor: Martijn Claes

Certificatieprogramma Beveiliging IoT

Deze template is een goede basis om je onderzoek goed voor te bereiden en nadien uit te voeren.

# Situering

Deze masterproef gebeurt in samenwerking met de afdeling Digital Testing van de firma Eurofins. Deze afdeling doet onder andere kwaliteitstesten en probeert nu om ook beveiligingstesten op de markt te brengen. De opgave bestaat er in een plan te ontwikkelen om de beveiliging van IoT-devices te testen. Dit is noodzakelijk omdat er een IoT-apparaat in elk aspect van ons dagelijkse leven gaat verschijnen. Zonder waterdichte beveiliging zou de gebruiker zijn volledige levensstijl kunnen gevolgd worden, zouden botnets kunnen gemaakt worden die de hele internetstructuur van kleinere landen kunnen onbruikbaar maken, en zou kritieke informatie in de verkeerde handen kunnen terechtkomen.

# Probleemstelling (onderzoeksvragen)

De testen die nu gebeuren worden ad hoc bepaald, en dekken zeker de volledige lading van beveiligingsrisicos niet. Deze testen moeten aangevuld worden, en in een plan geplaatst worden zodat eender welk IoT device kan doorgelicht worden, en zoveel mogelijk geautomatiseerd met behulp van scripts en software.

# Doelstellingen

Het doel van dit onderzoek is een testplan op te stellen dat kritieke beveiligingsrisico’s opspoort.  
Dit testplan moet zoveel mogelijk voorkomen dat IoT-devices op de markt komen die kwetsbaar zijn voor afluisteren van dataverkeer, foutief toekennen van hoge privileges, en uitvoering van schadelijke code. Dit testplan is best van beperkte duur, bijvoorbeeld 5 dagen.

# Materiaal en methode

# In eerste plaats zal worden nagegaan op welke manieren IoT-devices veelal communiceren.

Hierbij wordt vooral gefocust op de communicatieprotocollen, de beveiligingsprotocollen en –algoritmen, en de ingebedde microprocessoren. Hierop volgend zal, op basis van door andere instanties al opgestelde criteria, een analyse worden gemaakt van de belangrijkste testen die moeten worden uitgevoerd.

Uiteindelijk zal op zoveel mogelijk van de punten uit de genoemde analyse een testplan ontwikkeld worden, dat de beveiliging moet controleren. Dit testplan zal zoveel mogelijk toekomstbestendig geformuleerd worden, en zal zelf ook getest worden, tussentijds met een gecontroleerde testopstelling, en een finale versie met een IoT-device waarvan één- of meerdere zwakheden gekend zijn.

# Timing/planning

