Onderzoeksopzet:

# 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 to brengen. De opgave bestaat er in een plan te ontwikkelen om de beveiliging van IOT-devices te testen. Het belang van de beveiliging van “smart”-apparaten bestaat eenvoudigweg in de hoeveelheid ervan de producenten denken te verspreiden. Gezien er milioenen huishoudens in België zijn, de meest primitieve internetverbinding nog een dataverkeer van een megabit per seconde kan onderhouden, en er gemiddeld tussen tien en honderd van dergelijke apparaten kan verwacht worden per huishouden, zou zonder degelijke beveiliging eenvoudigweg tera- of zelfs peta-bits per seconde aan dataverkeer kunnen worden aangewend om internet-diensten lam te leggen.

# Probleemstelling:

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-apparaat kan doorgelicht worden, en zoveel mogelijk geautomatiseerd met behulp van scripts en software. Over het algemeen moet de analyse in 3 domeinen gebeuren: Het netwerk en webdomein niveau, het firmware niveau, en het fysieke apparaat. Omdat in het eerstgenoemde domein al heel veel gekend is, wordt dit domein in dit onderzoek veelal achterwege gelaten.

# Doelstellingen:

Het doel van dit onderzoek is een testplan op te stellen dat kritieke beveiligingsrisicos opspoort.  
Dit testplan moet zoveel mogelijk voorkomen dat IOT-apparaten op de markt komen die kwetsbaar zijn voor afluisteren van dataverkeer, foutief toekennen van hoge privileges, en uitvoering van vreemde code. Dit testplan moet zo ontwikkeld zijn dat het niet langer dan 5 werkdagen duurt om uit te voeren.

# Methode:

In eerste plaats zal worden nagegaan op welke manieren IOT-apparaten veelal communiceren. Er zal een vooronderzoek gebeuren waarin wordt nagegaan op welke manier de IOT devices communiceren met de buitenwereld. Hierbij wordt vooral gefocust op het communicatie-medium, kanaal-en-broncodering, encryptie, en de gebruikte (micro)processoren.  
  
Hierop volgend zal, op basis van door andere instanties al opgestelde Common Criteria, een analyse worden van de belangrijkste delen van de beveiliging die getest moeten worden.

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 verzie met een IOT-device waarvan één- of meerdere zwakheden gekend zijn.