Introductie:   
We beginnen met een Fermi oefening om het belang aan te tonen van het fatsoenlijk beveiligen van IoT-apparaten: Er zijn 10^6 huishoudens in België, waarvan ervan uit gegaan wordt dat van elk huishouden 10^0 devices kan gebot worden, en zonder op te vallen 10^5 bits per seconden kan afgetapt worden, die vervolgens met een factor 10^2 versterkt worden door NTFS-spoofing. Dit maakt een DDoS-aanval van 10^13 bits per seconde. Ter vergelijking: De grootste DDoS aanval die tot dusver bijgehouden is, de aanval op de servers van Github in maart 2018, had 1.35 \* 10^12 bits per seconde als piek dataverkeer.  
  
Met andere woorden: als IoT-apparaten slecht beveiligd worden, kunnen DDoS aanvallen zo buiten proportie groeien dat ze niet alleen gelijk welke service, maar mogelijk zelfs het internet zelf kunnen lam leggen. Het belang van de beveiliging kan dus niet genoeg onderstreept worden, zeker gezien er nu al malware zoals Mirai specifiek op IoT wordt losgelaten. Omdat de IoT-markt voorlopig nog heel versnipperd is, en elk bedrjif zijn eigen beveiliging voorziet, kunnen er gemakkelijk problemen over het hoofd gezien worden. Eurofins Digital Testing probeert daarom een dekkend testplan te ontwikkelen om deze apparaten op vlak van beveiliging door te lichten, om op deze manier er toch voor te kunnen zorgen dat zo weinig mogelijk vergeten wordt.