# Opdracht

|  |
| --- |
| **Context:**  De beveiliging van computer- en software-systemen vormt een complex domein. Uiteraard zijn er de studies van technische aspecten zoals crypto-algoritmes en -protocollen, browsers, programmeertalen. Cybersecurity wordt echter meer en meer ook bestudeerd vanuit een speltheoretische invalshoek (<http://en.wikipedia.org/wiki/Game_theory>). In essentie is de interactie tussen misbruikers en beschermers van systemen een 'spel', waarbij de verschillende partijen beslissingen moeten nemen. Daartoe wordt door de partijen een inschatting gemaakt van bv. de intenties en computationele capaciteiten van de andere, en van de gevolgen die beslissingen met zich kunnen meebrengen. Eén voorbeeld is de nasleep van Heartbleed. Door het grootschalig gebruik van SSL zijn de gevolgen bij het detecteren van beveiligingsproblemen enorm groot. Verschillende partijen (website-eigenaars, gebruikers, ISPs, etc.) 'interageren' hierbij in die zin dat hun individuele beslissingen over hoe hiermee om te gaan (patches, aanpassen wachtwoorden, afsluiten websites, etc.) een effect hebben op het globale probleem en oplossing. Het is een belangrijke analyse om te achterhalen wat de gevolgen van deze beslissingen zijn, zodat ook kan worden bestudeerd welke incentives moeten worden gecreëerd (en door wie) om de partijen díe beslissingen te laten nemen die voor globaal betere bescherming zorgen.  Een ander voorbeeld (uit Proc. of GameSec conference, 2010) is de studie van beveiligingsproblemen door middel van botnets bij websites die gebruik maken van Ad Networks. De vraag stelt zich welke partij zich in welke mate moet beschermen, en welke de kosten zijn die men hiervoor wil dragen. Zo zijn ISPs best geschikt om aanvallen of misbruiken te erkennen en te remediëren, maar beschouwen zij het veelal niet als hun verantwoordelijkheid, en bovendien staat hier een aanzienlijk kost tegenover die zij niet willen of kunnen dragen. De Ad Networks zijn vragende partij om de problemen aan te pakken, maar zijn niet goed geplaatst om dit te doen. Een speltheoretische analyse bouwt een aantal assumpties, maakt geschikte modellen op, en maakt een voorstel voor afspraken tussen ISPs en de Ad Networks.    Speltheorie is nl. de wetenschappelijke studie van strategische interactie, en beschrijft het gedrag van rationele spelers die hun opbrengst proberen te maximaliseren. Speltheorie is gegrond in wiskunde en in de economische wetenschappen, maar wordt ook onderzocht binnen computerwetenschappen. Daar is het een populair onderwerp binnen de context van competitieve multi-agent systemen, computersystemen die bestaan uit meerdere interagerende, autonome, zelfzuchtige softwareagenten. Softwareagenten stellen vaak entiteiten voor uit de echte wereld, zoals bijvoorbeeld autobestuurders die deel uit maken van het weggennet en die het plannen van hun route uitbesteden aan hun GPS systeem. |
| **Doel:**  In deze masterproef stel je, in samenspraak met begeleider en promotor, zelf een relevant scenario voor waarbij beslissingen m.b.t. beveiliging genomen dienen te worden, maar waarbij het strategisch karakter van de interactie een eenvoudige oplossing in de weg staat (zoals Heartbleed, Ad Networks, etc). Je gaat daarna een geschikte speltheoretische modellering en analyse uitvoeren, om daaruit de nodige strategische conclusies te trekken. |
| **Mogelijke Onderzoeksvragen:**   * Voor welke situaties binnen een context van beveiliging vormt speltheorie een goeie, gefundeerde uitvalsbasis voor analyse? * Welk speltype is geschikt voor het modelleren van een gekozen situatie? * Onder welke omstandigheden is een analytische dan wel een experimentele methode de meest geschikte voor analyse van een spelsituatie? |

# RQ uit eerste versie van Sophies text

This an lead us to the following research questions:

* Is it possible to incorporate the notion of delay in the game-theoretical analysis of the Flip-It game ?
* Is it possible to incorporate the notion of delay in the game-theoretical analysis of the Flip-It game ?
* Does this allow us to determine an optimal defense strategy against an attacker? for example: Gaat er een specieke grootte zijn van een delay waarbij de attacker al weet dat hem niet meer moet gaan spelen ? ( is niet gelijk aan de grootte van de periode van de attacker)

Resarch questions when working with a network and a delay: .. graph model en uitleggen hoe we de graph kunnen maken zodat de delay altijd zo groot mogelijk gaat zijn.

* How can we calculate the expected duration for a node’s infection/the entire network infection ?
* Can we calculate this node per node ?

Doel:

In deze masterproef stel je, in samenspraak met begeleider en promotor, zelf een relevant scenario voor waarbij beslissingen m.b.t. beveiliging genomen dienen te worden, maar waarbij het strategisch karakter van de interactie een eenvoudige oplossing in de weg staat (zoals Heartbleed, Ad Networks, etc). Je gaat daarna een geschikte speltheoretische modellering en analyse uitvoeren, om daaruit de nodige strategische conclusies te trekken.

# Ontwerp mail 2 ivm doelstellingen.

Beste Jonathan,

Omdat de tijd dat ik nog aan mijn thesis kan besteden eindig is, en om mijn tijd efficiënt te kunnen besteden, is het voor mij belangrijk heel doelgericht te kunnen werken. Ik wil daarom toch graag de doelstellingen kennen voor het afwerken van mijn thesis om de juiste prioriteiten te kunnen zetten.

Wat de delays betreft (punt 3 uit mijn mail), heb je in je mail van 11 mei, waarin je een aangepaste structuur voor de thesis voorstelt, een hoofdstuk 5 over ‘determining delays’ in de outline opgenomen. Mijn vraag is gewoon om te bevestigen dat dit een literatuurstudie moet zijn in de plaats van het eerste voorstel (berekening via matrix).

Punten 1 en 2 uit mijn mail werk ik sowieso uit. Tijdens de vergadering kwam ter sprake of het al of niet wenselijk is de formules verder uit te breiden naar de niet-periodische situatie, maar ik begreep uit de reactie van Kristof (Kristof kan dit al dan niet bevestigen) dat dit niet realistisch is en dus buiten de scope van de opdracht van een masterproef ligt.

Het uitwerken van de periodische situatie ligt in lijn met de oorspronkelijke opdracht, waarin wordt gevraagd om ‘een’ relevant scenario uit te werken en daarvoor een speltheoretisch model op te stellen.

Ik kan alleen maar beamen dat het idee dat het bekijken van het periodische geval weinig is, een verkeerde inschatting is. Ik heb daar vele uren aan besteed, en het is niet omdat er nu een formule ligt, dat die poepsimpel te vinden was. De inspanning die geleverd is tijdens de zoektocht is moeilijk tastbaar te maken, tenzij ik alle logisch lijkende maar foute alternatieven uitschrijf.

Ik ben het niet mee eens dat dit ‘achteraf’ zou bekeken worden. Mijn vraag is hoe dit gaat vastgesteld worden ? Op basis van welke informatie ? Ik wil graag nu weten wat de concrete criteria zijn waarop ik zal geëvalueerd worden. Ik begrijp dat de eindscore ook afhankelijk is van de tekst en de verdediging, maar ik wil nu graag de bevestiging dat ik geen extra formules moet uitwerken. Ander is het doel een “moving target” en dan is het onmogelijk om doelgericht en gemotiveerd te werken.

Vriendelijke groeten,

Sophie