Speltheorie en cybersecurity: een studie van het verdedingen van netwerken 1337

Iedereen heeft wel al eens gehoord van het volgende spelletje: een munt opgooien en raden of de munt valt op de zijde met kop of de zijde met munt. Degene die het bij het juiste eind heeft, wint de munt. Dit is een voorbeeld van een spel dat kan geanalyseerd worden via speltheorie. In speltheorie wordt er gezocht naar de beste tactiek van een speler. In het spel van kop-of-munt zijn er dus twee spelers die elk de juiste zijde van een opgegooide munt willen raden om het spel te winnen. Hierbij is de taktiek zeer eenvoudig. De helft van de tijd kop gokken en de andere helft munt van de tijd munt gokken. Er zijn ook spellen waarbij de taktiek wat ingewikkelder ligt. We kunnen dit toelichten via een ander zeer bekent spel in de speltheorie namelijk het gevangenis dilemma. In het gevangenis dilemma zijn er twee spelers die beide rationeel zijn en beide een misdaad begaan hebben. Rationeel betekent dat ze het beste voor zichzelf willen en het niet hun doel is om de ander kwaad aan te doen. Allebei zitten ze opgesloten in een apart lokaal en weten niet van elkaar wat ze gaan vertellen. Elk van hen kan de ander verraden of ze kunnen elkaar steunen en blijven zwijgen. Als een speler bekent krijg hij afhankelijk van wat de andere doet, drie jaar gevangenis of hij is vrij om te gaan. Als de speler zwijgt krijg hij afhankelijk van wat de andere speler doet ofwel vijf jaar gevangenis ofwel een jaar. (Dit is verduidelijkt op figuur 1). De beste strategie is om allebei te zwijgen, maar perfect rationele spelers kiezen er toch voor om allebei te bekennen. Dit levert hen drie jaar gevangeis op in plaats van een jaar. Waarom spelers dit doen kan uitgelegd worden aan de hand van speltheorie.

Speltheorie is dus in het algemeen een studie van mathematische modellen van rationele spelers die willen samenwerken of niet-samenwerken. Het is pas in opgang gekomen gedurende de tweede wereldoorlog met Oskar Morgenstern en John von Neumann die beide een boek publiceerden over speltheorie, getiteld “Theory of Games and Economic Behaviour“ (De speltheorie en economisch gedrag) in 1944. Later volgde er een boek dat speltheorie toepaste op de economie. John Nash speelde ook een grote rol in de geschiedenis van de speltheorie. Het Nash evenwicht werd naar hem vernoemd. Een Nash equilibrium wordt gezien als een evenwicht tussen beide spelers zodat ze allebei de beste tactiek kiezen en niet meer veranderen als de andere van tacktiek veranderen. John Nash breide het Nash evenwicht in een paper nog uit met gemengde strategiën.

{{[Robert Axelrod](http://nl.wikipedia.org/w/index.php?title=Robert_Axelrod&action=edit&redlink=1) wilde in 1979 middels een wedstrijd uitvinden welke strategie het beste werkte bij herhaalde [gevangenendilemma](http://nl.wikipedia.org/wiki/Gevangenendilemma)’s. [Anatol Rapoport](http://nl.wikipedia.org/wiki/Anatol_Rapoport) heeft voor deze wedstrijd het systeem 'tit for tat' ontwikkeld. Op grond van dit systeem vond hij een schijnbaar optimum voor het gevangenendilemma door steeds coöperatief te handelen, behalve als de ander niet-coöperatief handelde. Dit systeem gold jarenlang als de beste oplossing tot het in 1993 werd vervangen door de theorie van [Martin Nowak](http://nl.wikipedia.org/w/index.php?title=Martin_Nowak&action=edit&redlink=1) en [Karl Sigmund](http://nl.wikipedia.org/w/index.php?title=Karl_Sigmund&action=edit&redlink=1). Deze gaat ervan uit dat je dezelfde strategie moet volgen als in de vorige zet wanneer die tot een gunstig resultaat leidde en moet wisselen van strategie wanneer dit niet het geval was }} Over John Nash is een prachtige film gemaakt, “A Beautiful Mind”.

Speltheorie kan op verschillende domeinen toegepast worden. Denk maar aan politiek, economie, biologie, sociologie … en ook security. Security is het geheel van middelen die ingezet worden om een doel te beveiligen tegen kwaadaardige bedreigingen. Cybersecurity is een onderdeel van security en focust zich op het beveiligen van computergestuurde apparaturen zoals computers en smartphones en dergelijke, evenals computer netwerken zoals publieke en private netwerken, met inbegrip van het hele internet. Het is het nemen van maatregelen om integriteit, confidentialiteit en beschikbaarheid van data te garanderen. Dat betekent dat er de zekerheid wordt gegeven dat data niet wordt verwijderd zonder toelating, dat de data altijd toegankelijk is en dat de data niet wordt gelezen of gewijzigd door iemand die hier geen toegang toe heeft. Om te weten hoe een systeem verdedigd moet worden is het belangrijk om de verschillende manieren te kennen van hoe een systeem aangevallen kan worden. Een van de manieren om een systeem of computer aan te vallen is door het gebruik van malware. Malware is een slecht stuk programma dat gaat proberen om op onbeveiligde systemen of computers binnen te geraken en daar aan gevoelige informatie te geraken. Virussen, wormen, trojans zijn voorbeelden van malware.

Om beter te weten hoe een systeem of computer kan verdedigd worden tegen aanvallers kan men speltheorie gebruiken. Het spel dat gemodeleerd word is een spel tussen twee spelers, de verdediger en de aanvaller. De verdediger kan de netwerk manager zijn die het netwerk van een bedrijf zal moeten verdedigen. De aanvaller kan een programeur zijn die virussen schrijft om een netwerk van een bedrijf aan te vallen. In dit artikel bespreken we een bepaald model om een spel te modelleren namelijk FlipIt. FlipIt is een spel dat bedacht is door onder andere Rivest, de man die aan de basis stond van RSA. Met FlipIt wordt er een spel gespeeld tussen twee spelers, de verdediger en de aanvaller. Beiden willen ze de controle krijgen over een gemeenschappelijke resource. Deze resource kan bijvoorbeeld een wachtwoord, een computer of een volledig netwerk zijn. De spelers kunnen de controle krijgen door de resource te flippen. Met flippen wordt er een actie uitgevoerd door een van de spelers om controle te krijgen over de resource. Dus als de defender de resource flipt dan heeft hij de controle over de resource. Als de attacker dan de resource flipt dan verliest de defender de controle over de resource en heeft de attacker nu de controle over de resource. Een flip kan op elk moment gebeuren. De spelers moeten niet tegelijkertijd spelen of eerst wachten op een actie van de andere speler. Ze zijn vrij in het kiezen van wanneer ze spelen. Elke flip houdt wel een bepaalde kost in. FlipIt is een spel dat oneindig lang doorgaat. Het doel van het spel is om de tijd te maximaliseren dat ze de resource in bezit hebben en de kost te minimaliseren. Het unieke aan FlipIt wat het anders maakt als de andere spellen in de speltheorie is dat het flippen “stealthy” gebeurt. Er wordt dus geheimlijk geflipt, dat betekent dat de andere niet weet wanneer zijn tegenspeler de controle over de resource probeert te nemen. Het kan voorvallen dat de attacker bijvoorbeeld denkt dat hij de controle over de resource kwijt is en een flip doet terwijl hij toch nog de controle over de resource heeft. Dit wordt dan een “flop” genoemd omdat dit een verloren kost inhoud.

FlipIt is een handig spel om bepaalde dingen te gaan modelleren. Wat we gaan proberen te modeleren is de propagatie van wormen en virussen in een netwerk model. De scoop van het netwerk model zal een bedrijfsnetwerk zijn. Veel netwerken van bedrijven moeten zich op een continue tijd verdedigen tegen indringers van buitenaf zoals virussen en wormen. Ze willen hun netwerk zo clean mogelijk. Als er dan toch een indringer is geslaagd om het netwerk binnen te dringen dan wilt de netwerk manager deze indringer zo snel mogelijk buitenkrijgen. Dit is niet altijd even makkelijk. Zeker niet wanneer de indringers geheimlijk binnenglippen en zich dan snel verspreiden. Het “I love you” virus is een voorbeeld van een virus dat zich snel verspreid. Dit virus verspreid zich via mail. Als iemand de mail opende met het I-love-you virus in dan kon dit virus zichzelf verspreiden door een mail te sturen met zichzelf naar iedereen in de contactlijst. Zo kon het virus zich heel snel verspreiden en kon uiteindelijk het netwerk van een bedrijf platleggen. Het platleggen gebeurde omdat er teveel verkeer was op het netwerk. Teveel pakketten gingen over en weer en uiteindelijk kan een netwerk dit niet meer aan en kan er niets meer geleverd worden. In dit voorbeeld was er een menselijke interactie nodig om het virus te doen verspreiden. Als niemand de mail opend dan kan het virus zich niet verspreiden. Jammer genoeg zijn er ook virussen die zich kunnen verspreiden zonder dat er iemand anders helpt. Deze virussen worden wormen genoemd. Een worm is ook een stukje slechte code die zich een weg baand van computer tot computer. De Stuxnetworm is een zeer bekende worm. Het starte met zich te verspreiden via geinfecteerde USB sticks en vanaf dan kon het zich via het internet verspreiden naar andere computers. Het doel van de Stuxnetworm was om kernreactoren kapot te laten draaien. Vele kernreactoren zijn geinfecteerd geweest en plat gelegd. Vanuit de verdediger zijn standpunt is het dus zeer belangrijk om zo snel mogelijk te reageren zodat de worm zich niet snel kan verspreiden.

Via FlipIt kunnen we deze situatie gaan modelleren. Hiervoor worden er een aantal aanpassingen aan FlipIt gedaan. De enkele resource wordt nu vervangen door meerdere resourcen. Deze gaan het netwerk van een bedrijf modelleren. De resources zullen computers voorstellen van de werknemers in het bedrijg. De verbinden/linken tussen de resources zijn logische linken die de verbinding via email moeten voorstellen. Dus als een werknemer een andere werknemer is zijn contactlijst heeft staan dan zullen de twee computers van deze werknemers verbonden zijn. Er zijn ook twee mogelijkheden voor het flippen. De ene mogelijkheid is om te “onderzoeken”. Dat betekent dat de resource nog niet geflipt wordt, maar er gegeken wordt wie de controle heeft over de resource. De andere mogelijkheid is het “recoveren” en dat betekent dat het virus of de worm verwijderd wordt maar de resouce is wel nog steeds onbeschremd tegen een tweede aanval van het virus. De kost voor het “onderzoeken” is minder groot dan de kost voor het “recoveren”. Dat zou dus kunnen betekenen dat het misschien meer voordeliger is om eerst na te kijken en pas daarna het virus of de worm te verwijderen als de computer effectief geinfecteerd is.

We gaan dus via FlipIt onderzoeken wat de beste strategien zijn voor de defender en de attacker.

Wat moet er instaan:

Introductie tot Speltheorie

Verband met security malware → Worm

Introductie tot FlipIt

Veranderingen aan het model FlipIt

Hoe het gemoduleerd wordt