**Speltheorie en cybersecurity:**

**een studie van het verdedigen van netwerken**

Door Sophie Marien

**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 gemodelleerd worden via speltheorie.** In speltheorie wordt de strategische interactie tussen de spelers bestudeerd. 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. Als beide spelers kop gokken of allebei munt gokken dan is het gelijkspel en wint niemand. Er kan alleen gewonnen worden als de andere speler fout gokt. Om de grootste kans te krijgen om te winnen moet de speler de helft van de tijd kop gokken en de andere helft munt van de tijd munt gokken. Er zijn ook spellen waarbij de winnende tactiek 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 hebben begaan. 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 ze 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 hieronder).



Figuur 1: Gevangenisdilemma

**Bekennen Zwijgen**

**Bekennen Zwijgen**

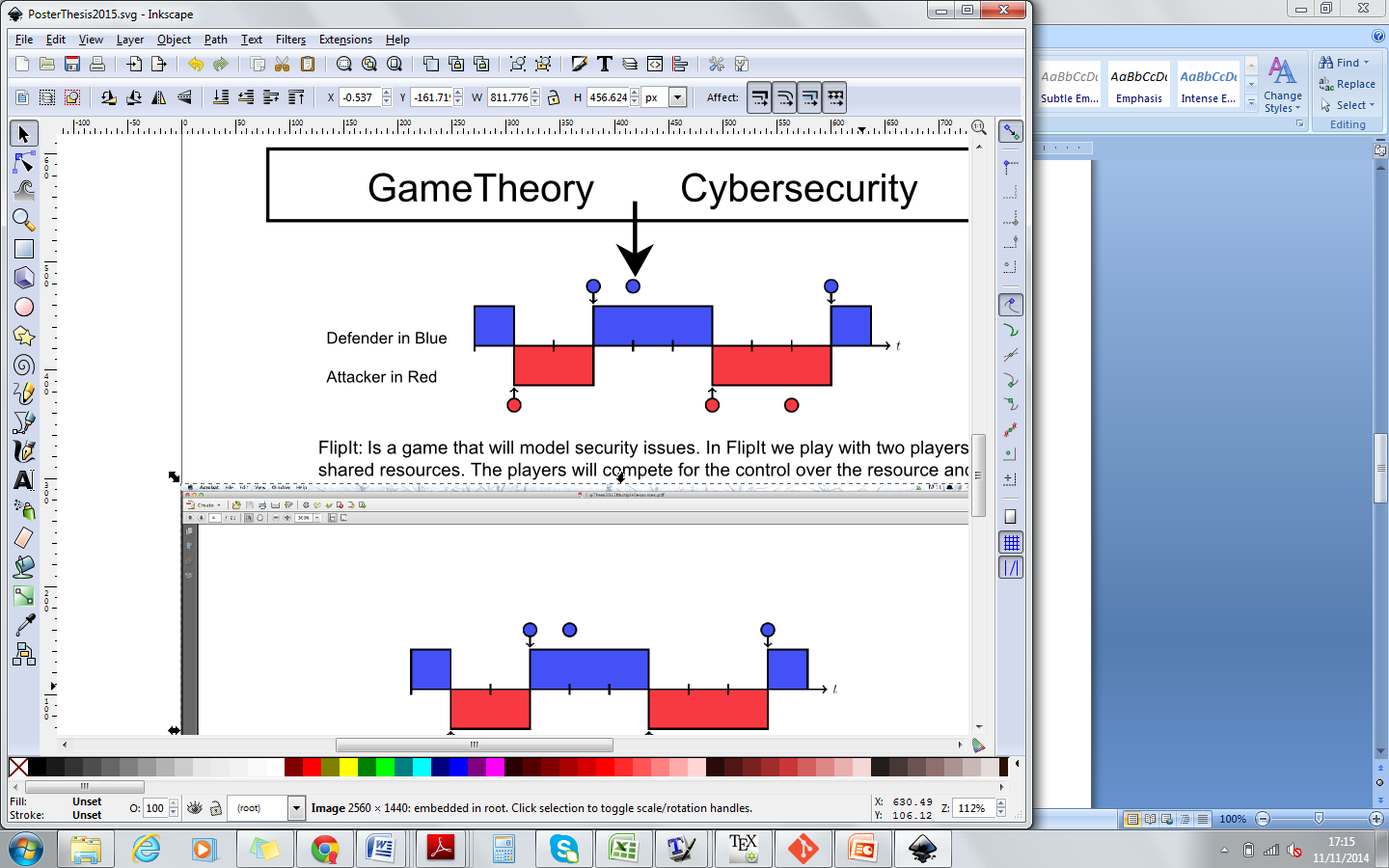
De beste strategie is om allebei te zwijgen, maar perfect rationele spelers kiezen er toch voor om allebei te bekennen. Dit levert hen drie jaar gevangenis op in plaats van een jaar. Waarom spelers dit doen kan uitgelegd worden aan de hand van speltheorie.

GESCHIEDENIS 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. Dit boek handelde over de wiskundige analyse van een reeks denkspelen. Hierin werd er een onderscheid gemaakt tussen spelen waarin de strategieën en de utility factor van de tegenstander geen invloed heeft op het vinden van de beste strategieën zoals schaken en spelen waarbij dit wel een invloed heeft zoals poker. John Nash speelde ook een grote rol in de geschiedenis van de speltheorie. Hij is een van de wiskundigen geweest die speltheorie geformaliseerd heeft. Het Nash evenwicht werd naar hem vernoemd. Een Nash evenwicht wordt gezien als een evenwicht tussen beide spelers zodat ze allebei de beste tactiek kiezen en niet meer veranderen als de andere van tactiek veranderen. John Nash breide het Nash evenwicht in een paper nog uit met gemengde strategieën. In 1994 kreeg John Nash samen met twee andere wiskundigen gespecialiseerd op het vlak van speltheorie de Nobelprijs voor de economie op basis van hun prestaties in de niet-coöperatieve speltheorie. In 1979 is er een wedstrijd opgesteld geweest om uit te vinden welke strategie het beste is bij herhaalde gevangenisdilemma’s. Anatol Rapoport heeft deze wedstrijd gewonnen met zijn ‘tit for tat’ systeem. Hierbij vond hij een schijnbaar optimum voor het gevangenisdilemma door steeds coöperatief te handelen, tenzij de tegenspeler niet coöperatief handelt. Jarenlang was dit systeem de beste oplossing tot er in 1993 twee wiskundigen, Martin Nowak en Karl Sigmund een andere strategie vonden. Bij deze strategie moet de speler dezelfde strategie volgen als de vorige zet wanneer deze tot een gunstig resultaat geleid heeft en wisselen van strategie als dit niet het geval was. Over John Nash is een prachtige film gemaakt, “A Beautiful Mind”.

SPELTHEORIE EN CYBERSECURITY

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.



Figuur 2: FlipIt

FLIPIT

Om beter te weten hoe een systeem of computer kan verdedigd worden tegen aanvallers kan men speltheorie gebruiken. Het spel dat gemodelleerd wordt 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 programmeur zijn die virussen schrijft om een netwerk van een bedrijf aan te vallen.

In dit artikel bespreken we een bepaald model om dit soort spelen te modelleren namelijk FlipIt. FlipIt is een spel dat bedacht is door onder andere Rivest, de man die aan de basis stond van RSA. FlipIt is een spel dat gespeeld wordt door twee spelers, de verdediger en de aanvaller. Beiden willen 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.. Dus als de verdediger de resource flipt dan heeft hij de controle over de resource. Als de aanvaller erna de resource flipt dan verliest de verdediger de controle over de resource en heeft de aanvaller 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. 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.

Wat FlipIt anders maakt dan de andere spelen in speltheorie is dat het flippen “stealthy” gebeurt. Er wordt dus geheimlijk geflipt, wat betekent dat de andere speler niet weet wanneer zijn tegenspeler de controle over de resource probeert te nemen. Het kan voorvallen dat een speler 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.

PROPAGATIE WORMEN EN VIRUSSEN

In dit artikel gaan we proberen om de propagatie van wormen en virussen in een netwerk model te modelleren via speltheorie. De scoop van het netwerk model is een bedrijfsnetwerk. Veel bedrijfsnetwerken moeten zich op een continue tijd verdedigen tegen indringers van buitenaf zoals virussen en wormen. De netwerk manager zal proberen het netwerk zo vrij mogelijk te houden. Als er dan toch een indringer is geslaagd om het netwerk binnen te dringen dan zal de netwerk manager deze indringer zo snel mogelijk proberen buiten te krijgen. 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 plant zich voort via mailsystemen. Als iemand een mail opent met het “I love you” virus in bijlage dan verspreidt dit virus zichzelf door een mail te sturen met zichzelf naar iedereen in de contactlijst. Zo kan het virus zich zeer snel propageren en uiteindelijk het netwerk van een bedrijf platleggen door het vele verkeer. In dit voorbeeld is er een menselijke interactie nodig om het virus te doen verspreiden. Als niemand de mail opent dan kan het virus zich niet verspreiden. Jammer genoeg bestaan er ook virussen die zich kunnen verspreiden zonder menselijke interactie. Deze virussen worden wormen genoemd. Een worm is ook een stukje slechte code die zich repliceert om zich zo te verspreiden naar andere computers. Meestal gebruikt een worm een computer netwerk om zich te verspreiden en zal het gebruik maken van beveiligings failures om andere computer te infecteren. De meeste wormen worden gemaakt om zich alleen maar te verspreiden en proberen geen veranderingen te brengen aan de systemen die ze passeren. Deze wormen kunnen nog steeds schade toebrengen door de verhoogde netwerk trafiek die ze genereren. Wormen die wel schade berokken bevatten een programma om een “backdoor” te installeren of een “rootkit” op deze geïnfecteerde computers. De “backdoors” en “rootkits” zorgen ervoor dat er later gebruik kan gemaakt worden van de geïnfecteerde computers. De Stuxnetworm is een zeer bekende worm. Het startte met zich te verspreiden via geïnfecteerde 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 geïnfecteerd 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.

FLIPIT MET MEERDERE RESOURCES

Via FlipIt kunnen we deze situatie gaan modelleren en analyseren. Hiervoor worden er een aantal aanpassingen aan FlipIt gedaan. De eerste aanpassing is dat de enkele resource wordt vervangen door meerdere resourcen. Deze stellen de noden voor in het netwerk van een bedrijf. De noden zullen computers voorstellen van de werknemers in het bedrijf. De verbinden/linken tussen de noden zijn logische linken die de connectie via email moeten voorstellen. Dus als een werknemer een andere werknemer in zijn contactlijst heeft staan dan zullen de twee computers van deze werknemers verbonden zijn in het noden netwerk. Door tweede aanpassing zijn er twee verschillende mogelijkheden om een node te flippen. De ene mogelijkheid is om te “onderzoeken”. Dat betekent dat de resource nog niet geflipt wordt, maar er gekeken 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. Dit betekent niet dat de resource beschermd is tegen een tweede aanval. Het kan nog steeds geïnfecteerd worden. De kost voor het “onderzoeken” is minder groot dan de kost voor het “recoveren”. Dit zou kunnen betekenen dat het misschien meer voordeliger is om eerst na te gaan of de node geïnfecteerd is en pas daarna recoveren als het effectief geïnfecteerd is. Een derde aanpassing is de kost voor de aanvaller en de verdediger. Als de aanvaller teveel noden tegelijkertijd flipt en over een bepaalde treshholdwaarde gaat dan komt de verdediger te weten dat er een virus zich aan het propageren is. Het flippen gebeurt nog steeds geheimlijk alleen is de verdediger nu bewust van het feit dat er een aanvaller is. Via FlipIt gaan we onderzoeken wat de beste strategieë­­­­­n zijn voor de verdediger en de aanvaller. ­­Welke noden in het netwerk moeten frequenter geflipt worden en welke worden er beter onderzocht voordat er onmiddelijk gerecoverd wordt. Andersom voor de aanvaller, hoe frequent moet de aanvaller aanvallen en welke noden zijn goede target noden. De aanvaller moet ook mee rekening houden dat als er teveel nodes tegelijkertijd geflipt worden, de kans groter is dat er opgemerkt kan worden dat er een virus/worm zich op het netwerk bevindt.