

SPELTHEORIE EN CYBERSECURITY

Een studie over strategieën voor het verdedigen van bedrijfsnetwerken

Sophie Marien

Virussen zijn een groot probleem voor bedrijfsnetwerken. Ze kunnen gevoelige informatie verzamelen of een bedrijfsnetwerk platleggen. Gegeven de grote kost gebonden aan schade door malware, is het vinden van de juiste verdedigingsstrategie belangrijk. Het aanvallen en verdedigen van een bedrijfsnetwerk kan gezien worden als een spel, waarbij de verdediger en de aanvaller elk proberen de beste strategie te vinden. In dit artikel lichten we toe hoe het spel van aanvallen en verdedigen kan gedefinieerd worden als een variatie op het spel FlipIt. Dit laat toe om te onderzoeken wat de verschillende strategieën zijn van de netwerkbeheerder enerzijds en van de aanvaller die virussen zendt anderzijds. De bedoeling is om in een volgende stap het spel verder te analyseren met behulp van speltheorie om te bepalen welke de dominerende strategieën zijn en of er zich Nash equilibria voordoen.

Security is het geheel van middelen die ingezet worden om een doel te beveiligen tegen kwaadaardige bedreigingen. Deze bedreigingen variëren van virussen die programma's installeren, tot het lekken van vertrouwelijke informatie of een programma voor een '*denial of service*' attack. De jaarlijkse kost voor een bedrijf aan security kan hoog oplopen en daarom is het dus belangrijk voor een bedrijf om de juiste verdedigingsstrategie te vinden.

CYBERSECURITY

In dit artikel concentreren we ons op cybersecurity. Cybersecurity is een onderdeel van security en focust zich op het beveiligen van computergestuurde apparaten zoals computers en smartphones, evenals computernetwerken

zoals publieke en private netwerken, met inbegrip van het hele internet. Een privaat netwerk zoals een bedrijfsnetwerk wordt afgeschermd van het publiek netwerk zoals het internet. Het doel van beveiliging is zekerheid te geven dat data niet wordt verwijderd zonder toelating (confidentialiteit), dat de data altijd toegankelijk is (beschikbaarheid) en dat de data niet wordt gelezen of gewijzigd door iemand die hier geen toelating voor heeft (integriteit).

Om te weten hoe een systeem verdedigd moet worden, is het belangrijk om te weten hoe het aangevallen kan worden. Een van de manieren om een systeem of computer aan te vallen is door gebruik te maken van malware. Dit is een kwaadwillig stuk programma dat zal proberen





om onbeveiligde systemen of computers binnen te dringen en daar aan gevoelige informatie te geraken. Virussen, wormen, trojans zijn voorbeelden van malware.

SPELTHEORIE EN CYBERSECURITY

Speltheorie kan op verschillende domeinen toegepast worden. Denk maar aan politiek, economie, biologie, sociologie ... en ook op het domein van security. Speltheorie bestudeert de strategische interactie tussen de spelers in een spel. In een spel kunnen er een aantal spelers zijn die elk acties kunnen uitspelen. Deze acties zijn voorgesteld door een getal dat hun voorkeur aangeeft.

GEVANGENEN DILEMMA

Een voorbeeld van een spel met twee spelers is bijvoorbeeld het gevangenisdilemma. In dit spel zijn er twee spelers die beiden rationeel zijn en

		P2	
		Talk	Stay Silent
P1	Talk	 3 YEARS 3 YEARS	 FREE 5 YEARS
	Stay Silent	 5 YEARS FREE	 1 YEAR 1 YEAR

Figuur 1: Het gevangenisdilemma: P1 komt overeen met de eerste kolom, P2 met de tweede kolom.

beiden een misdaad hebben begaan. 'Rationeel zijn' 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 bekend, krijgt 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.

SPELTHEORIE KAN OP VERSCHILLENDE DOMEINEN TOEGEPAST WORDEN .. OOK OP HET DOMEIN VAN SECURITY

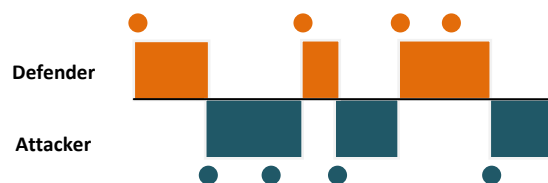
Figuur 1 toont de verschillende combinaties van de mogelijke acties van de twee spelers. Het Nash equilibrium (zie verder) van het spel is dat ze allebei zwijgen, maar perfect rationele spelers kiezen er toch voor om allebei te bekennen. Dit komt omdat dit de dominante strategie is. Een dominante strategie is een strategie die beter is als alle andere strategieën van een speler onafhankelijk van de tegenspeler. Hier is het voor elke speler voordeliger om te bekennen. Dit levert hen drie jaar gevangenis op in plaats van een jaar. Waarom spelers voor de ene of de andere actie kiezen kan uitgelegd worden aan de hand van speltheorie.

Door speltheorie te gebruiken kan men uitzoeken hoe een netwerk het best kan verdedigd worden tegen aanvallers. Het spel dat gemodelleerd wordt, is een spel tussen twee spelers: de verdediger en de aanvaller. De verdediger kan de netwerkmanager zijn die het netwerk van een bedrijf zal moeten verdedigen. De aanvaller kan een programmeur zijn die virussen schrijft om een netwerk van het bedrijf aan te vallen.

FLIPIT

In dit artikel bespreken we een bepaald model om dit soort spelen te modelleren, met name Fliplt (figuur 2). Fliplt 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. Er moet ook rekening mee gehouden worden dat elke flip een bepaalde kost inhoudt. Fliplt is een spel dat oneindig lang doorgaat. Het doel van het spel is voor elke speler om de tijd dat hij de *resource* in bezit heeft te maximaliseren en zijn kost te



Figuur 2: Fliplt

minimaliseren. Wat Fliplt anders maakt dan de andere spelen in speltheorie is dat het flippen *stealthy* gebeurt. Er wordt dus heimelijk geflipt, wat betekent dat de andere speler niet weet wanneer zijn tegenspeler de controle over de *resource* probeert over 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 inhoudt.

Een kleine toepassing van Fliplt is het beschermen van een *resource* via een wachtwoord. Wanneer de aanvaller het wachtwoord reset, wat overeenkomt met een flip, heeft hij bezit over de *resource*. De verdediger kan dit terug flippen door weer het wachtwoord te resetten. Geen van beide spelers weet wanneer de andere het wachtwoord gereset heeft.

VAN FLIPIT NAAR CYBERSECURITY

Veel bedrijfsnetwerken moeten zich continu verdedigen tegen indringers van buitenaf zoals virussen en wormen. De netwerkbeheerder zal proberen het netwerk zo malware-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 heimelijk binnenglippen en zich dan snel verspreiden.

Cybersecurity vertoont dus gelijkenissen met het spel Fliplt. Het flippen komt overeen met het overnemen van de controle over (een deel van) het netwerk. Het gebeurt ook heimelijk en continu. Toch zijn er ook verschillen, te wijten aan de complexiteit van de verschillende vormen van malware. Virussen hebben verschillende manieren om zich te verspreiden en verschillen ook in de schade die ze willen toebrengen.

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 vermenigvuldigen 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 computerprogramma dat zich dupliceert om zich zo te verspreiden naar andere computers. Via een computernetwerk worden kopieën van de worm doorgestuurd zonder dat er een tussenpersoon voor gebruikt wordt. De worm zal gebruikmaken van beveiligingslekken om andere computers te infecteren.

De meeste wormen worden gemaakt om zich

WORMEN ZIJN VIRUSSEN DIE ZICH KUNNEN VERSPREIDEN ZONDER MENSELIJKE INTERACTIE

alleen maar te verspreiden en proberen geen veranderingen aan te brengen aan de systemen die ze passeren. Deze wormen kunnen nog steeds schade toebrengen door de verhoogde netwerktrafiek die ze genereren. Wormen die wel schade berokken bevatten een programma om een *backdoor* te installeren of een *rootkit* op de 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. Initieel verspreide deze worm zich via geïnfecteerde USB sticks en vanaf dan kon het

zich via het internet verspreiden naar andere computers. Het doel van de Stuxnetworm was om de centrifuges in kernreactoren kapot te laten draaien. Vele kernreactoren zijn geïnfecteerd geweest. Vanuit het standpunt van de verdediger is het dus zeer belangrijk om zo snel mogelijk te reageren zodat de worm zich niet snel kan verspreiden.

AANPASSINGEN AAN FLIPT

Om via Flipt een situatie van aanvallen van virussen en wormen te modelleren zijn er dus een aantal aanpassingen aan Flipt nodig.

De eerste aanpassing is dat de enkele *resource* wordt vervangen door meerdere *resources*. Deze stellen de knooppunten voor in het bedrijfsnetwerk. Elk knooppunt is een computer van een werknemer in het bedrijf. De verbindingen (linken) tussen de knooppunten zijn de logische communicatieverbindingen, zoals de contactpersonen in een mailinglijst van de computer. Er wordt van uitgegaan dat als de ene computer iemand in zijn contactlijst heeft staan dat de andere deze ook in zijn contactlijst heeft staan zodat de linken bidirectioneel zijn.

De tweede en laatste aanpassing is een extra actie voor de spelers. In plaats van te flippen is het nu ook mogelijk om te “onderzoeken”. Dat betekent dat de *resource* nog niet geflipt wordt, maar er gekeken wordt wie de controle heeft over de *resource*. De kost voor het “onderzoeken” is minder groot dan de kost voor het flippen. Dit zou kunnen betekenen dat het misschien voordeliger is om eerst na te gaan of een knooppunt geïnfecteerd is en pas daarna flippen als het knooppunt effectief geïnfecteerd is. Wat onveranderd blijft is dat het flippen en het “onderzoeken” steeds heimelijk gebeurt en dat het spel in een continue tijd doorgaat.

Op een gegeven moment zal de aanvaller een virus sturen of plaatsen op een van de knooppunten via bijvoorbeeld een USB stick. De verdediger zal ten alle tijden proberen zijn netwerk *clean* te houden. Vanaf dat moment zal het virus zich gaan verspreiden over de andere knooppunten. De propagatiestrategie van het virus is vooraf bepaald. Dat betekent dat de propagatie snelheid vast ligt en de actie van het virus.

Het virus heeft twee acties die het kan uitspelen. De ene actie is dat het onmiddellijk alle knooppunten waarmee het in verbinding staat gaat infecteren. De andere actie is dat het virus telkens maar één knooppunt kan infecteren. Het virus kan voor deze actie kiezen om minder snel opgemerkt te worden. Een geïnfecteerd knooppunt kan maar een keer al zijn naburige knooppunten infecteren. Een variatie op deze twee acties is dat het al dan niet een wederkerige actie kan zijn. Dit betekent dat een geïnfecteerd knooppunt zijn aanvaller terug kan infecteren. Hierdoor kan dit knooppunt terug al zijn burens infecteren.

De verdediger heeft één belangrijke actie: het flippen of “onderzoeken” van een bepaald aantal knooppunten per keer. De kost van het aantal knooppunten stijgt op een progressieve

SPELTHEORIE IS TOEPASBAAR BINNEN CYBERSECURITY

manier zodat de verdediger niet als triviale zet alle knooppunten flipt. Voor een verdediger is het de bedoeling om het bedrijfsnetwerk *clean* te houden op een zo goedkoop mogelijke manier omdat hij over een bepaalde tijd binnen een budget blijven. Een variatie op deze actie is dat de verdediger ervoor kan kiezen om de knooppunten in groep of onafhankelijk van elkaar te flippen. De enige speler die vooraf aan de start van het spel informatie heeft, is de verdediger. Deze heeft kennis van de topologie van het netwerk.

VERDER ONDERZOEK

Voor het verdere onderzoek kunnen we via Flipt analyseren wat de dominante en optimale verdedigingsstrategieën zijn voor de verdediger en aanvallingsstrategieën van de aanvaller. Er kan ook onderzocht worden of het spel een Nash equilibrium heeft. Speltheorie is dus toepasbaar binnen cybersecurity en Flipt leent zich voor speltheoretische analyse van cybersecurity.

Nash Equilibrium en John Nash

John Nash speelde een grote rol in de geschiedenis van de speltheorie. Hij is een van de wiskundigen geweest die speltheorie geformaliseerd heeft. Het Nash equilibrium 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 tactiek veranderen. John Nash breide de theorie over het Nash equilibrium 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. Over John Nash is een prachtige film gemaakt, “A Beautiful Mind”.