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 elks 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 Game Theory om te bepalen welke de dominerende strategieën zijn en of er zich Nash equilibria (zie verder) voordoen.

Security is een belangrijk punt waar aandacht aan moet besteed worden. 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 van een bedrijf aan security kan hoog oplopen en daarom is het dus belangrijk voor een bedrijf om de juiste verdedigingsstrategie te vinden.

CYBERSECURITY

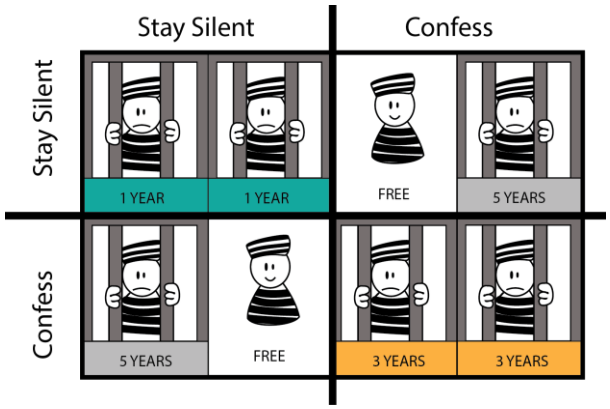
In dit artikel gaan we ons concentreren op cybersecurity. Cybersecurity is een onderdeel van security en focust zich op het beveiligen van computergestuurde apparaten zoals computers en smartphones, evenals computernetwerken zoals publieke en private netwerken, met inbegrip van het hele internet. Het is het nemen van maatregelen om de integriteit, confidentialiteit en beschikbaarheid van data te garanderen. Het doel van beveiliging is zekerheid te geven 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 hoe het aangevallen kan worden. Een van de manieren om een systeem of computer aan te vallen is door het gebruik van malware. Dit is een kwaadwillig stuk programma dat gaat proberen om op 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. In speltheorie wordt de strategische interactie tussen de spelers in een spel bestudeerd. Een spel wordt gespeeld door een aantal spelers en elk van deze spelers heeft acties. Deze acties worden voorgesteld door een getal die hun voorkeur aangeeft.



Figuur 1: Het gevangenisdilemma

GEVANGENIS 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 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 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.

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

Op figuur 1 worden de voorkeuren van elke gevangene weergegeven. Het Nash equilibrium 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 eene of de andere actie kiezen kan uitgelegd worden aan de hand van speltheorie.

Door speltheorie te gebruiken kan men beter weten hoe een systeem of computer 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 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.

FLIPIT

In dit artikel bespreken we een bepaald model om dit soort spelen te modelleren namelijk FlipIt (figuur 2). 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.

Figuur 2: FlipIt

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 inhoud. 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 heimlijk 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 inhoud.

VAN FLIPIT NAAR CYBERSECURITY

In dit artikel gaan we proberen om de propagatie van wormen en virussen in een netwerk model te modelleren via speltheorie. De scope van het netwerk is een bedrijfsnetwerk. Veel bedrijfsnetwerken moeten zich op een continue tijd 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 heimlijk binnenglippen en zich dan snel verspreiden.

WORMEN ZIJN VIRUSSEN DIE ZICH KUNNEN VERSPREIDEN ZONDER MENSELIJKE INTERACTIE

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 computerprogramma dat zich repliceert om zich zo te verspreiden naar andere computers. Via een computernetwerk worden copieën van de worm doorgestuurd zonder dat er een tussenpersoon voor gebruikt wordt. Het zal gebruikmaken van beveiligingslekken om andere computer te infecteren.

De meeste wormen worden gemaakt om zich 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 skernreactoren 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 FLIPIT

Via FlipIt kunnen we een situatie van aanvallen van virussen en wormen gaan modelleren en analyseren. Hiervoor zijn er een aantal aanpassingen aan FlipIt nodig.

De eerste aanpassing is dat de enkele resource wordt vervangen door meerdere resources. Deze stellen de noden voor in het bedrijfsnetwerk. Elk van deze node is een computer van een werknemer in het bedrijf. De verbindingen (linken) tussen de noden zijn de logische communicatieverbindingen, zoals de contactpersonen in een maillinglijst van de computer. Er wordt vanuitgegaan 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 aanpassing en laatste is een extra actie voor de spelers. In plaats van te flippen is

Nash Equilibrium en John Nash

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 de theorie over 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. . Over John Nash is een prachtige film gemaakt, “A Beautiful Mind”.

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 de node geïnfecteerd is en pas daarna recoveren als de node effectief geïnfecteerd is. Wat onveranderd blijft is dat het flippen en het “onderzoeken” steeds heimlijk gebeurt en dat het spel in een continue tijd doorgaat.

Op een gegeven moment zal de aanvaller een virus droppen op een van de nodes. De verdediger zal ten alle tijden proberen zijn netwerk clean te houden. Vanaf dat moment zal het virus zich gaan verspreiden over de andere nodes. De propagatiestrategie van het virus is vooraf bepaald.

Het virus heeft twee acties dat het kan uitspelen. De ene actie is dat het onmiddelijk alle noden waarmee het in verbinding staat gaat infecteren. De andere actie is dat het virus telkens maar een node kan infecteren. Het virus kan voor deze actie kiezen om minder snel opgemerkt te worden. Een geinfecteerde node kan maar een keer al zijn naburige noden infecteren. Een variatie op deze twee acties is dat het al dan niet een wederkerende actie kan zijn. Dit betekent dat een node die aangevallen is zijn aanvaller terug kan infecteren. Hierdoor kan deze node terug al zijn buren infecteren.

De verdediger heeft één belangrijke actie: het flippen of onderzoeken van een bepaald aantal noden per keer. De kost van het aantal noden stijgt op een progressieve manier zodat de verdediger niet als triviale zet alle nodes flipt. Voor een verdediger is het de bedoeling om het bedrijfsnetwerk clean te houden op een zo goedkoop mogelijke manier. Een variatie op deze actie is dat de verdediger ervoor kan kiezen om de noden in groep te flippen of onafhankelijk van elkaar. De enige speler die vooraf het spel informatie heeft is de verdediger. Die heeft kennis van de topologie van het netwerk.

VERDER ONDERZOEK

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