With the significant growth of the Internet, more and more individuals and companies are relying on it.

Growth of the Internet → more vulnerabilities → necessary to secure

Defenders try to build secure solutions against the attacks → variation

Game theory is an approach that can help to understand the threats and to model the strategy of a defender or an attacker. With this model it can describe the interactions between these two players and guess which defender strategy is the best to play.

Game theory can help to model the strategy of a defender . It is a way to describe the interactions between an attacker and a defender.

→ when patching or reorganizing

Short introduction to game theory

Game theory is not about games such as computer games or board games. Game theory is a way of modeling strategic interactions between self-interested players. Self-interested players means that they only care about themselves and have no intention to hurt the other player. They have their own description of the state of the world as they like it. Every interaction will have a level of happiness. Utility function. This will be interpreted as the state of the world as they like.

For further details the reader is referred to [] .

A player has a set of possible actions, with these actions utility functions and the tuples of actions are the outcome. The utility function represents the preferences of the player for a given action. For the formal game the players play simultaneously.

Example : Prisoners dilemma

Nash equilibrium

“The basic assumption of game theory is that

every player acts rationally, aiming at the best possible outcome, and take into account

other players’ decisions. Solution to a game is the description of the strategies that each

player has to follow in order to achieve the best possible outcome. Nash equilibrium is

the solution of the game that describes a steady state, where each player gets the best

possible payoff. A deviation from the Nash Equilibrium strategy always leads in lesser

payoff. ” [] 3 various categories: Cooperative games- non cooperative games, static-dynamic and perfect – imperfect games, complete-incomplete games, and pure – mixed strategies.

Rationality

Normal Form Games → players move as if simultaneous

Extensive Form Games → players move sequentially, represented as a tree

players can be people, governments, companies, armies..

Introduction to FlipIt (pratical bv cryptografic keys or passwords)

First an explanation about FlipIt. FlipIt is a two-players game with a shared (single) resource that the players want to control as long as possible. We will call the players the Attacker and the Defender. To get the control over the resource the players can flip the resource. This will happen in a stealthy way, meaning that the other player has no clue that the other player has flipped the resource. Both players can move at any given time. A move will have a cost. The goal of the game is to have the most control over the resource with a minimal total cost. “The attacker can take over the resource at any given time. The only option for the defender is to retake over by moving later again. The game will go on for ever. “ [Slides FlipIt]

“A player learns the state of the system only

when she moves.

 In basic FLIPIT, each move has feedback that

reveals all previous moves.

 (In variants, move reveals only current state, or

time since other player last moved...)”

Categories Classes of Strategies

Non-adaptive (NA) Exponential Periodic

Renewal

General non-adaptive

Adaptive (AD) Last move (LM)

Full history (FH)

Stealthy

continuously

Idee: Defender moet een subset van resources kiezen om een critical attack uit te voeren. De attacker mag maar 1 resource kiezen van de set van resources om aan te vallen. Elke resource heeft een kost. De defender heeft een budget waaraan hij minimaal moet voldoen. Ofwel gaat de defender meerdere resources kiezen met een kleinere kost (de kost is dus ook kleiner om die terug over te nemen) ofwel kiest de defender mindere resources met een grotere kost.

Nog uitvinden wanneer ze elke keer mogen aanvallen

Welke van de twee tactieken is het beste (minder of meer resources)

Toepassing: Leger die servers gaat gebruiken om een aanval uit te voeren. Maar ze hebben ook fake servers geplaatst die de aandacht moeten trekken van attackers.

Of ook een netwerk voor transport. Heel node netwerk. Pad vinden en die nodes gebruiken. Topology van de andere is treelike

TO Read:

Markov model

Game Theoretic Approach for Cost-Benefit Analysis of

Malware Proliferation Prevention?

Worm

Worm is different from a virus.

The shared resource is something sensitive like password, node in a network, ..

Because of the significant growth of the internet, malware is been one of the predominantly threats of interconnected computers. Malware, another word for malicious software, compromises viruses, Trojan Horses, worms, spyware, adware and other malicious software. The aim is to exploit existing vulnerabilities to gain access to private systems or steal sensitive data. Some of the malicious software may harm .. other not ..

Well known worms: Stuxnet, CodeRed, SQL Slammer,

Propagation

POPULARISEREND ARTIKEL

(intro te kinderachtig, ander voorbeeld zoeken, mss met geld, of de kop of munt, of het prisoners dilemma) .

Ooit eens een moeilijke keuze gehad dat afhing van wat je vriend zou kiezen ? Er is een taart en die wordt verdeeld in 10 stukken. Jij en je vriend mogen allebij tegelijkertijd zeggen hoeveel stukken taart je wil hebben. Als de som van de stukken die je vriend wilt en die jij wilt kleiner of gelijk is aan 10 stukken dan mogen jullie de stukken hebben. Is de som van alle stukken groter dan krijgen jullie niets. Jullie willen allebij natuurlijk taart hebben en liefst zoveel mogelijk dus gaan jullie zo een antwoord proberen te geven zodat jullie allebij taart hebben en zo veel mogelijk. Dit soort spelletjes is Gametheory. In Gametheory gaan we proberen te zoeken naar het best mogelijke antwoord met het beste resultaat voor alle spelers. We noemen dit resultaat ook nog wel het Nash Equilibrium. Nash was een belangrijke man in de gametheorie. Hij probeerde the utility functie voor iedereen te maximaliseren. (niet elk spel heeft een Nash equilibrium).

Nu we weten wat gametheory is gaan we dit toepassen op cybersecurity. Cybersecurity is het helpen beveiligen van het internet tegen malware,.. .. Malware is eigenlijk een slecht stuk programma dat gaat proberen om op onbeveiligde computers binnen te geraken en daar aan gevoelige informatie te geraken. Er zijn al verschillende soorten defentie mechanismen die de malware onder bedwang willen houden. Gametheory kan hierbij helpen om het gedrag te modeleren van beide spelers. De beide spelers in het spel zijn de verdediger en de attacker.

#### Rocra malware: unique architecture and functionality

The attackers created a multi-functional attack platform that includes several extensions and malicious files designed to quickly adjust to different systems’ configurations and harvest intelligence from infected machines. The platform is unique to Rocra and has not been identified by Kaspersky Lab in previous cyber-espionage campaigns. Notable characteristics include:

* “Resurrection” module: A unique module that enables the attackers to “resurrect” infected machines. The module is embedded as a plug-in inside Adobe Reader and Microsoft Office installations and provides the attackers a foolproof way to regain access to a target system if the main malware body is discovered and removed, or if the system is patched. Once the C2s are operational again the attackers send a specialized document file (PDF or Office document) to victims’ machines via e-mail which will activate the malware again.
* Advanced cryptographic spy-modules: The main purpose of the spying modules is to steal information. This includes files from different cryptographic systems, such as [Acid Cryptofiler](http://fr.wikipedia.org/wiki/Acid_Cryptofiler), which is known to be used in organizations of NATO, the European Union, European Parliament and European Commission since the summer of 2011 to protect sensitive information.
* Mobile Devices: In addition to targeting traditional workstations, the malware is capable of stealing data from mobile devices, such as smartphones (iPhone, Nokia and Windows Mobile). The malware is also capable of stealing configuration information from enterprise network equipment such as routers and switches, as well as deleted files from removable disk drives.

Populariserend Artikel

Wat moet er instaan:

Introductie tot Speltheorie

Verband met security malware → Worm

Introductie tot FlipIt

Veranderingen aan het model FlipIt

Hoe het gemoduleerd wordt

Iedereen heeft het spelletje wel al eens gespeeld: een munt opgooien en de ene zegt kop en de andere munt. Degene die het juist raad op welke zijde de munt valt 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 de munt heb je dus twee spelers die elk de juiste zijde van een munt willen raden om het spel te winnen. Een ander zeer bekent spel in de speltheorie is het gevangenis dilemma. In het gevangenis dilemma heb je twee rationele spelers die 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. Ze worden allebei opgesloten in een apart lokaal en weten niet van elkaar wat ze gaan vertellen. Elk van hen kan de ander verraden of ze kunnen zwijgen. Als een speler bekent krijg hij afhankelijk van wat de andere doet, 3 jaar of hij is vrij. Als de speler zwijgt krijg hij ofwel 5 jaar ofwel 1 jaar in de gevangenis. Ook al is de beste keuze om allebei te zwijgen zullen perfect rationele spelers er toch voor kiezen om allebei te bekennen. Dit levert hen 3 jaar op ipv 1 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 met John von Neumann die een paper publiceerde over speltheorie. Later volgde er een boek die speltheorie toepaste op de economie. John Nash speelde ook een grote rol in de geschiedenis van de speltheorie. Hij kwam op met de term Nash equilibrium. 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. Over John Nash is een prachtige film gemaakt, “A Beautiful Mind”.

Speltheorie kan op verschillende domeinen toegepast worden. Denk maar aan politike, economie, … en ook security. Met security wordt hier bedoeld het helpen van het beveiligen van het internet tegen malware. Malware is eigenlijk een slecht stuk programma dat gaat proberen om op onbeveiligde computers binnen te geraken en daar aan gevoelige informatie te geraken. Er zijn al verschillende soorten defensie mechanismen die de malware onder bedwang willen houden. Denk maar aan firewalls, adware, .. Gametheory kan hierbij helpen om het gedrag te modelleren van beide spelers. De beide spelers in het spel zijn de verdediger en de aanvaller. Een probleem kan op verschillende manier gemodelleerd worden door speltheorie. In dit artikel bespreken we een bepaald model van speltheorie 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 controle krijgen over een gemeenschappelijke resource. Ze kunnen dit doen door de resource te flippen. 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 de andere. Ze zijn vrij in het kiezen van wanneer ze spelen. Elke flip houdt wel een bepaalde kost in. Op het einde is het doel om de tijd te maximaliseren dat ze de resource in bezit hebben en de kost te minimaliseren. Het speciale aan FlipIt wat het anders maakt als de andere spellen in de speltheorie is dat het flippen “stealthy” gebeurd. 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 dus ook gebeuren 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. Vele netwerken van bedrijven moeten zich heel de 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 werd doorgegeven 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.

VERANDERINGEN AAN FLIPIT/FLIPTHEM

– De attacker krijgt een voorsprong

– Meerdere resources → subset van de resources die meer dan de helft is dan is er controle over

– Scope is een netwerk binnen een bedrijf

DEFENDER

Flippen Hoe?

→ Flipt alleen wanneer hij ontdekt heeft dat er een worm zich propageert

→ Dus Defender heeft voorkennis

→ Flipt resources

1. Ofwel meerdere resources tegelijk (subset te bepalen)

→ Moet een tijd wachten voordat er terug opnieuw een subset kan geflipt worden.

→ Kost voor elke flip is groot (groter dan enkele flip)

2. Ofwel maar 1 flip per keer

→ Kan sneller herhaald worden van subset van resources flippen

→ kost is niet zo groot

ATTACKER

Flippen Hoe ?

→ Flipt op een gegeven tijdsstip

→ Weet niets van de tacktiek van de Defender

→ Flipt aan de start 1 resource

→ Verdere propagatie zijn er twee mogelijkheden

1. Ofwel flipt deze onmiddellijk een subset van resourcse.

→ Doet dit na enige tijd terug opnieuw

→ Eerste Flip is gewone kost, tweede kost is duurder

2. Ofwel elke keer maar 1 resource flippen.

→ Kans dat dezelfde resources terug geflopt wordt

→ Kost is elke keer gelijk

→ Kan sneller flippen, dan het subset flippen

Geen Patchen meer.

VRAGEN:

\* Welke taktiek is beter voor de attacker? De subset flippen of elke keer een resource flippen.

\* Welke taktiek onderdrukt het snelst de worm bij de defender ?

\* ...

Stel via mail dan wordt topologie de logische topologie van de computers die aan elkaar verbonden zijn via contacten in de mail.

## Scope ?

Netwerk van een bedrijf:

Netwerk(Internet)

fysiek geconnecteerd

Vragen gesteld over netwerkbeheer in het bedrijf OneAccess en wat er gebeurt wanneer er en virus/zwrom is:

Ongeveer 600 pc’s voor een middelgroot bedrijf.

Gebruik van firewall om controle te hebben over de inkomende en uitgaande communicatie.

Stel virus/worm:

* Patchen gebeurt door rond te gaan met een usb stick
* Computer wordt uit het netwerk gehaald
* Soms wordt computer gewoon vervangen
* Bv I love You virus: wisten welke pc’s besmet waren, die warden afgesloten van het network

Meestal verspreid een virus/worm zich zeer snel.

Komt binnen via attachment mail, download van web, http request..

Meestal firewall van DMZ zone alleen controle op fysische en netwerklaag (af en toe transportlaag). Dus virussen en wormen die via applicatieniveau binnenkomen worden niet gefilterd door de firewall. (bv poort 80 staat altijd open ). Er bestaan ook firewalls die op applicatieniveau binnenkomen maar die zijn zeer duur. (7000 euro).