KU LEUVEN
FACULTEIT INGENIEURSWETENSCHAPPEN

Gametheory and Cybersecurity: a study FlipIt and multiple resources

Sophie Marien

Thesis voorgedragen tot het behalen
van de graad van Master of Science
in de ingenieurswetenschappen:
computerwetenschappen,
hoofdspecialisatie Veilige software

Promotor:
Prof. dr. ir. Tom Holvoet

Assessoren:
Ir. W. Eetveel
W. Eetrest

Begeleider:
Ir. Jonathan Merlevede, Ir. Kristof
Coninx

Academiejaar 2014 – 2015

Voorwoord

I would like to thank everybody who kept me busy the last year, especially my promotor and my assistants. I would also like to thank the jury for reading the text. My sincere gratitude also goes to my wive and the rest of my family.

Sophie Marien

Inhoudsopgave

Voorwoord **i**

Samenvatting **iv**

Samenvatting **v**

Lijst van figuren en tabellen **vi**

List of Abbreviations and Symbols **vii**

1 Introduction **1**

1.1 Introduction 1

2 Intoduction to GameTheory **3**

2.1 A brief introduction in Game Theory 3

2.2 The FlipIt game 5

2.3 Extensions on FlipIt 8

3 FlipIt game with virus propagation **11**

3.1 Introduction 11

3.2 FlipIt game with virus propagation 11

3.3 Explaining difference between FlipIt with and without virus propagation 11

3.4 Formal definition Game 13

3.5 Benefit for FlipIt game with virus propagation 14

3.6 something 15

3.7 Simulation 17

4 Virus Propagation **19**

4.1 Methods of virus propagation 19

4.2 REpresenting Virus Propagation in a network 19

A The First Appendix **25**

A.1 More Lorem 25

B The Last Appendix **27**

B.1 Lorem 20-24 27

Todo list

waarom? : lekken van informatie: je hebt info over klanten en moet hun privacy beschermen, je eigen data is geld waard voor concurrenten, DOSS attacks: je will je service-level agreements kunnen nakomen, ... 1

APT uitleggen ? en dat het moeilijk is om een systeem te beschermen tegen APT ==> overgang naar de volgende paragraaf maken. 1

Coursera 3

ref 3

leyton2008essentials 3

ref 3

ref 3

uitleggen aan de hand van een voorbeeld 3

players rationeel en max outcomes 3

strategien en acties definieren 4

Nash beter uitleggen nog met best response erbij 4

verwijzen naar de figuur 2.1 5

misschien meer uitleggen 8

citatie needed voor Are We Compromised? 9

bedrijven hebben niet het geld en de mankracht om zich daar mee bezig te houden en dan is periodisch verdedigen het handigste, bedrijven willen alles zo efficient en met de minste kost doen 11

voorbeeld geven van zo een worm 12

feit uit security rapport symantec 13

waarom geen patch, wormen kunnen veranderen gaandeweg 13

andere mogelijkheid: 13

Samenvatting

There are many possible ways to attack a company network. Everyday they suffer frrom multiple attakcs and stealthy attacks. We will make use of a gamemodel FlipIt to find out what the best strategies are for a network manager to defend his network. A worm or a virus will propagate through the network and will cause nodes to be infected. By flipping it the network manager can keep his network clean. In this thesis I present a work of gametheory merged with cybersecurity. The `abstract` environment contains a more extensive overview of the work. But it should be limited to one page.

Samenvatting

In dit `abstract` environment wordt een al dan niet uitgebreide Nederlandse samenvatting van het werk gegeven. Wanneer de tekst voor een Nederlandstalige master in het Engels wordt geschreven, wordt hier normaal een uitgebreide samenvatting verwacht, bijvoorbeeld een tiental bladzijden.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Lijst van figuren en tabellen

Lijst van figuren

2.1 A representation of a FlipIt game where both players are playing periodically and discrete. Every move or flip is indicated by a blue or orange circle. The attacker is the orange colour and plays with a period of $\delta_A = 4$. The defender is the blue colour and plays with a period of $\delta_D = 3$.The blue and orange rectangles represent the amount of time one of the players is in control of the resource. 5

Lijst van tabellen

2.1 Hierarchy of Classes of strategies in FlipIt 8

List of Abbreviations and Symbols

Abbreviations

LoG	Laplacian-of-Gaussian
MSE	Mean Square error
PSNR	Peak Signal-to-Noise ratio

Hoofdstuk 1

Introduction

1.1 Introduction

In this era where digitalization becomes prominent in every aspect of our lives, where technology is growing fast and where businesses are always under attack, security becomes an issue of increasing complexity. Without security, there is no protection to keep somebody out of a system. It is the same as leaving the door of your house wide open for everyone to come in. Why is it so important to keep a system secure? A hacker will be a person that seeks exploits or weaknesses in a system or network in order to gain access. Many of those attacks have a different cause. Some of the attacks by a hacker can be benign, others can be harmful. There are various ways to break into a system. Virusses, worms, spyware and other malware are the number two of the top external threats [security report kaspersky 2014]. Furthermore these kind of threats also causes the greatest percentage in loss of data. These threats will infect the network by means of a virus that will propagate through the network.

waarom? : lekken van informatie: je hebt info over klanten en moet hun privacy beschermen, je eigen data is geld waard voor concurrenten, DOSS attacks: je will je service-level agreements kunnen nakomen, ..

Since it is so difficult to protect a system or a network against APT, researcher have been looking for effective ways to predict in advance which defense strategy might be the better one. Game theory is gaining more and more interest as an effective technique to model and study Cyber Security. Game theory analyses the security problem as a game where the players are an attacker and a defender of a system, and where both players have to make decisions. In particular, both players will aim for the strategy that results in a maximal benefit for them. Researchers at RSA made a game theoretic framework to model targeted attacks. They study the specific scenario where a system or network is repeatedly taken over completely by an attacker and this attack is not immediately detected by the defender of the system or network. In game theory, such a game is known as ”FlipI”. This is a two players game where the attacker and the defender are competing to get control over a shared resource. Both players do not know who is currently in control of the resource until they move. In FlipIt every move gives them immediately control over the resource. But what if the attacker moves and it takes a while before the attacker gets full control over the resource? FlipIt does not take into account that a move may not be instantaneous, but has a certain delay. Consider for example a network with different

APT uitleggen ? en dat het moeilijk is om een systeem te beschermen tegen APT ==> overgang naar de volgende paragraaf maken.

nodes (laptops, datacenters) as a resource. The attacker drops a virus on one of the nodes and then wait till this virus infects the whole network. The attacker will only be in control of the resource once the whole network is infected.

The game theoretical approach of the FlipIt does not take such delay into account. This an lead us to the following research questions: - Is it possible to incorporate the notion of delay in the game-theoretical analysis of the Flip-It game ?

- Does this allow us to determine an optimal defense strategy against an attacker ? for example: Gaat er een specieke grootte zijn van een delay waarbij de attacker al weet dat hem niet meer moet gaan spelen ? (is niet gelijk aan de grootte van de periode van de attacker) When working with a network and a delay we can .. graph model en uitleggen hoe we de graph kunnen maken zodat de delay altijd zo groot mogelijk gaat zijn.

We propose an addition to the basic FlipIt model to model a scenario where the moves by the attacker will not be instantaneous. Next we analyse what the new Nash equilibria will be and ..

In the remainder of this thesis we

Hoofdstuk 2

Intoduction to GameTheory

Gametheory is a mathematical study to analyse interactions between independent and self-interested agents. To get an understanding of the most important concepts of game theory, a short introduction based on the work of [?] and is given in section 2.1 [] . For a more detailed and full introduction to game theory, the reader is referred to . In section 2.2 [] an overview of the FlipIt game is given with the definitions and concepts that will be used throughout the paper. The last section [] will cover the extensions and additions already made on FlipIt.

Coursera

ref

leyton2008essentials

ref

ref

2.1 A brief introduction in Game Theory

Game theory studies the interaction between independent and self-interested agents. It is a mathematical way of modelling the interactions between two or more agents where the outcomes depend on what everybody does and how it should be structured to lead to good outcomes. For this reason it can be very useful in economics and also in other branches as politics, biology, computer science, philosophy and a variety of other disciplines.

One of the assumptions underlying game theory is that the players of the game, the agents, are independent and self-interested. This does not necessarily mean that they want to harm other agents or that they only care about themselves. Instead it means that each agent has preferences about the states of the world he likes. These preferences are mapped to natural numbers and are called the utility function. The numbers are interpreted as a mathematical measure to tell you how much an agent likes or dislikes the states of the world.
It also explains the impact of uncertainty. When an agent is uncertain about a distribution of outcomes, his utility will describe the expected value of the utility function with respect to the probability of the distribution of the outcomes. For example: with 0.7 probability it will be 7 degrees outside and 0.3 probability it will be 10 degrees. The agent can have a different opinion about that distribution versus another distribution. ().
In a Decision Game Theoretic Approach an agent will try to act in such a way to

uitleggen aan de hand van een voorbeeld

players rationeel en max outcomes

maximise his expected or average utility function. It becomes more complicated when two or more agents want to maximise their utility and whose actions can affect each other utilities. This kind of games are referred to as non-cooperative game theory, where the basic modelling unit is the group of agents. The individualistic approach, where the basic modelling is only one agent, is referred as cooperative game theory.

In the following list a couple of terms that will be used throughout the paper.

Players: Players are referred as the ones who are the decision makers. It can be a person, a company or an animal. (they will act rational)

Actions: Every player has actions that he or he can do.

Strategies: A strategy is the combination of different actions. A pure strategy is only one action.

Utility function: The utility function is the mapping of the level of happiness of an agent about the state of the world to natural numbers.

A game in game theory consists of multiple agents and every agent has a set of actions that he can play.

strategien en acties definieren

2.1.1 Best response and Nash Equilibrium

One of the solution concepts in Game Theory for non-cooperative games is a Nash Equilibrium that we will use in this paper. A Nash Equilibrium is a subset of outcomes that can be interesting to analyse a game. For a Nash Equilibrium each player has a consist list of actions and each player's action maximizes his or her payoff given the actions of the other players. Nobody has the incentive to change his or her action if an equilibrium profile is played. In general we can say that a Nash Equilibrium is a stable strategy profile: each player is considered to know the equilibrium strategies of the other players and no player would want to change his own strategy if he knows the strategies of the other players.

Formal defenition of a Nash Equilibrium: A strategy profile $s = (s1, ..., sn)$ is a Nash equilibrium if, for all agents i, si is a best response to $s - i$. "Intuitively, a Nash equilibrium is a stable strategy profile: no agent would want to change his strategy if he knew what strategies the other agents were following. Wecan divide Nash equilibria into two categories, strict and weak, depending on whether or not every agent's strategy constitutes a unique best response to the other agents' strategies."

Nash beter uitleggen nog met best response erbij

POSTCONDITION: Uitgelegd: Strategien, acties, strategien, spelers, rationeel, Nash, best response

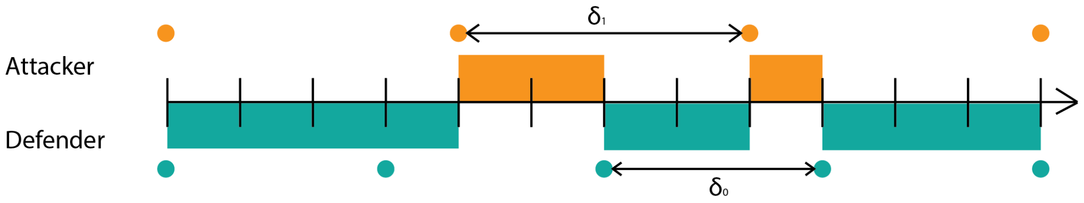
2.2 The FlipIt game

In this section, we introduce the ”stealthy takeover ” game FlipIt [**?**]. FlipIt is a game introduced by van Dijk et al. First we explain the framework of FlipIt and introduce the most important formules that will be used throughout the paper. To understand how to model a FlipIt game with virus propagation it is important to get familiar with the concepts of the normal FlipIt game and it’s notations.

FlipIt is a two-players game with a shared (single) resource that the players want to control as long as possible. The shared resource can be a password, a network or a secret key depending on the setting being modelled. In the rest of the paper we name the two players the attacker, denoted by the subscript A and the defender, denoted by subscript D.

The game begins at $t = 0$ and continuous indefinitely ($t \to \infty$). The time in the game can be viewed as being continuous, but a discrete time can also be viewed. To get control over the resource, the players i can flip the resource at any given time. A flip will be regarded as a move from a player i. Each move will imply a certain cost k_i and the cost can vary for each player. Both players will try to minimize their cost. By adding a cost, it will prevent players to move to frequently.

The unique feature of FlipIt is that every move will happen in a stealthy way, meaning that the player has no clue that (his adversary) the other player has flipped the resource. For instance, the defender will not find out if the resource has already been compromised by the attacker, but he can only potentially know it after he flips the resource himself. The goal of the player is to maximize the time that he or she has control over the resource while minimizing total cost of the moves. A move can also result in a "wasted move", called a flop. It may happen that the resource was already under control by the defender. If the defender moves when he or she has already control over the resource, he or she would have wasted a move since it does not result in a change of ownership and a cost is involved.



FIGUUR 2.1: A representation of a FlipIt game where both players are playing periodically and discrete. Every move or flip is indicated by a blue or orange circle. The attacker is the orange colour and plays with a period of $\delta_A = 4$. The defender is the blue colour and plays with a period of $\delta_D = 3$.The blue and orange rectangles represent the amount of time one of the players is in control of the resource.

verwijzen naar de figuur 2.1

The state of the resource is denoted as a time independent variable $C = C_i(t)$. $C_D(t)$ is either 1 if the game is under control by the defender and 0 if the game is under control by the attacker. For $C^A(t)$ it is visa versa, $C^A(t) = 1 - C^D(t)$.

The game starts with defender being in control of the game, $C_D(0) = 1$.

The players receive a benefit equal to the time of units that they were in possession of the resource minus the cost of making their moves. The cost of a player i is denoted by k_i. The total gain of player i is equal to the total amount of time that a player i has owned the resource from the beginning of the game up to time t. It is expressed as follows:

$$G_i(t) = \int_0^1 C_i(x)dx. \tag{2.1}$$

If we add up the gain of the defender and the gain of the attacker it should sum up to t:

$$G_D(t) + G_A(t) = t \tag{2.2}$$

The average gain of player i is defined as:

$$\gamma_i(t) = G_i(t)/t. \tag{2.3}$$

And thus for all $t > 0$:

$$\gamma_D(t) + \gamma_A(t) = 1 \tag{2.4}$$

Let $\beta_i(t)$ denote player's i average benefit upto time t:

$$\beta_i(t) = \gamma_i(t) - k_i\alpha_i. \tag{2.5}$$

This is equal to the fraction of time the resource has been owned by player i, minus the cost of making the moves. α_i defines the average move rate by player i up to time t. In a give game, the asymptotic benefit rate or simply benefit will be defined as the lim inf of the average benefit because time t will increase to infinity and the average benefit may not have limiting values.

$$\beta_i(t) = \lim_{t\to\infty} inf \beta_i(t)$$

strategies

Because the players move in a stealthy way, there are different types of feedback that a player can get while moving. These types of feedback can be divided into two groups of strategies. The non-adaptive strategies and the adaptive strategies. These are described in table 2.1.

If there is no need for feedback for both of the players, we say that we have a non-adaptive strategy. Because the player does not receive any feedback during the game it will play in the same manner against every opponent. They are not dependent on the opponents movements. This means that they can already generate the time sequence for all the moves in advance. But they can depend on some randomness because the non-adaptive strategies can be randomised. In this paper we will focus in the beginning on the non-adaptive strategies. Reasons behind this is that a player (defender or attacker) rarely knows what the strategies are of his opponent. An interesting subclass of the non-adaptive strategies is one where the time intervals between two consecutive moves are generated by a renewal process. Example of such a renewal strategy is the periodic strategy where the time between two consecutive moves of the players are a fixed interval. An exponential strategy is a renewal strategy in which the interval between two consecutive moves is exponentially distributed.

– Ik kan dit ook pas uitleggen als ik mijn FlipIt spel met virus propagatie uit de doeken doe –
We elaborate more about the periodic strategy because we will use this one to model our first extension. For more details about the other strategies of FlipIt we refer the reader to [the paper of FlipIt].

periodic strategy: A Periodic strategy is a non-adaptive renewal strategy where the time intervals between consecutive moves are a fixed period, denoted by δ. Moreover it has a random phase, that is chosen uniformly and random in the interval $[0, \delta]$ for the first move. The average rate of play is denoted by $\alpha = \frac{1}{\delta}$.

In the category Adaptive strategy there are two sub classes of strategies. The first one is the Last move (LM). In this class whenever a player flips it will find out the exact time that the opponent played the last time. In the second class the Full History (FH), whenever a player flips it will find out the whole history of the opponents move. If the opponent player plays with a renewal strategy the sub classes FH and LM collapse.
I

The game can be extended by the amount of information that a player receives. It can also be possible for a player to get information at the start of the game. Both interesting cases are:

- Rate-of-play (RP): The player finds out the exact rate of play of the opponent.
- Knowledge-of-strategy (KS): The player finds out the complete information of the strategy that the opponent is playing.

Imporant results

- periodische spellen domineren de andere renewal strategies
- periodische strategien wel slecht tegen attacker die laatste move weet
- als de defender snel speelt dan forceert die de attacker om niet meer mee te spelen

Categories	**Classes of Strategies**
Non-adaptive (NA)	Exponential
	Periodic
	Renewal
	General non-adaptive
Adaptive (AD)	Last move (LM)
	Full History (FH)

Tabel 2.1: Hierarchy of Classes of strategies in FlipIt

- iedereen die feedback krijgt heeft meer benefit dan zonder die feedback

2.3 Extensions on FlipIt

In this section we discuss the extensions that can be made on the FlipIt game.

There a various possible ways to extend FlipIt. Laszka et al. made a lot of additions and extensions on the original game of FlipIt. For instance Laszka et al. extended the basic FlipIt game to multiple resources. The incentive is that for compromising a system in a real case it needs more than just taking over just one resource. An example is that one resource can be gaining access to a system and breaking the password of the system is another resource. The model is called FlipThem [**?**]. They use two ways to flip the multiple resources: the AND and the OR control model. In the AND model the attacker only controls the system if he controls all the resources of the system, whereas in the OR model the attacker only needs to compromise one resource to be in control of the entire system.
Another addition of Laszka et al. to the game of FlipIt [mitigating covert compromises] is extending the game to also consider non-targeted attacks by non-strategic players. In this game the defender tries to maintain control over the resource that is subjected to both targeted and non-targeted attacks. Non-targeted attacks can include phishing, while targeted attacks may include threats delivered through zero day attack vulnerabilities.
One of the last important addition from Laszka et al. [Mitigation of Targeted and] is to consider a game where the moves made by the attacker are still covert but the moves made by the defender are known to the attacker. This means that the attacker can base his attacks on the defender's moves. Both the targeted and non-targeted attacks don't succeed immediately. For the targeted attack the time till it succeeds is given by an exponential distributed random variable with a known rate. The non-targeted attacks are modelled as a single attacker and the time till it succeeds is given by a Poisson process.. The conclusion of this paper is that the optimal strategy for the defender is moving periodically.

misschien meer uitleggen

Other authors used the FlipIt game to apply it on a specific scenario. To be able to use the FlipIt game, modifications where required for the FlipIt model. One of the scenarios by Pham[**?**] [] was to find out whether a resource was compromised or not by the attacker. This could be verified by the defender, who has an extra move "test"beside the flip move. The basic idea is to test with an extra action if the resource has been compromised or not. This move involves also an extra cost. This model is useful if somebody wants to know for example if his or her password has been compromised.

citatie needed voor Are We Compromised?

Finally researchers also have investigated the behavioural of humans when playing FlipIt. A Nochenson and Grossklags [A behavioural investigation of the FlipIt game] investigate how people really act when given temporal decisions. [Risk-seeking in a continuous game of timing] Reitter et al. they observe continuous games, 20-seconds FlipIt game..

Hoofdstuk 3

FlipIt game with virus propagation

3.1 Introduction

3.2 FlipIt game with virus propagation

Motivatie voor het veranderen van FLipIt naar een FlipIt met viruspropagatie:

3.3 Explaining difference between FlipIt with and without virus propagation

In chapter 2 the FlipIt game was explained. This chapter starts from the specific case of a non-adaptive continuous FlipIt game where both players play a periodic strategy with a random phase. This choice is motivated by the assumption that in the practical situation of most organisations, the defence strategy is to periodically defend the network. This corresponds to a periodic defender strategy. To simplify the analysis in a first time, a periodic attacker strategy is assumed as well. Further research can investigate the effect of relaxing this assumption.

bedrijven hebben niet het geld en de mankracht om zich daar mee bezig te houden en dan is periodisch verdedigen het handigste, bedrijven willen alles zo efficient en met de minste kost doen

A FlipIt game consists of a single resource. To represent the security problem, the game now defines its single resource as a computer network with multiple nodes. One of the players, the defender, will try to defend his network. The defender will do this by flipping all the nodes of the network (i.e. the entire resource) in every move he plays. The attacker, the other player, will try to infect all the nodes in the network. The attacker will do this by flipping the node in the graph that can infect all the nodes in the shortest time possible. After dropping a virus on the first node, it takes a while for the virus to infect the entire network. However, since the original FlipIt game works with a single resource that is always flipped entirely, the assumption is made that the attacker is considered to have gained the control over the resource only when all the nodes of the network have been infected, i.e. the entire resource has been flipped.

After dropping a virus on the first resource, it takes a while for the virus to infect the entire network. The time that it takes for the virus to infect every node will be denoted as parameter d. If we want to measure how long it takes for the virus to infect all the nodes in the network, we have to calculate the shortest path from the first infected node to the farthest node. This can be measured by a method that we will explain in section []. Assume that an attacker attacks at time t, then only at time t + d he gains control over the entire network. If the defender flips the network before the period d has elapsed (so, somewhere between t and t+ d), then the attacker will never gain control over the entire network. Using this parameter d, a FlipIt game with virus propagation can be modelled.

3.3.1 Actions of the attacker

A virus has different kind of ways of making his way through a company network. We will describe the different ways of how the virus can propagate. For start we will say that the virus or worm will be dropped on Node i and that it has k numbers of neighbours.

1. Node i is infected and will spread the virus or worm to every k neighbours and will stop infecting the neighbours in the next step
2. Node i is infected and will spread the virus or worm to every k neighbours and will keep on spreading the virus to the same neighbours in every next step
3. Node i is infected and will spread the virus to only one of the k neighbours and will stop infecting another neighbour in the next step
4. Node i is infected and will spread the virus to only one of the k neighbours and in the next step it will infect another one of the k neighbours

In the game that will be modelled in the paper we will use the settings of the first spreading method. We will not use method 2 because this kind of propagation will float the network. Because we use the settings of a mail system and contact in a mailing list the method of 3 and 4 are not used.

In the first method the node that has been infected can be again infected. If one of the neighbours infects the node again the node will infect his neighbours again. By using this spreading method we have three distinct states in which a node can be situated. An *infected state*, a *clean state* and a *spreading state*. An infected state means that the node is infected and will not spread the virus to its neighbours, a clean state means that the node is not infected on that moment and a spreading state means that the node is infected and that it will spread the virus or worm to its neighbours in the next step. We can argument this kind of propagation through a mail worm.

voorbeeld geven van zo een worm

The Attacker itself has two different ways of attacking the company network. It will only infected one node of the network and will wait for the virus to spread itself through the network. We will model two ways of attacks of an Attacker:

1. The attacker drops the virus on a random node on the network

2. The attacker drops the virus on a targeted node on the network

The attacker in this game will put a virus or worm on one of the nodes in the network. (This will happen at random.) The attacker does not know on which node the virus will be dropped. We will use this randomness because most viruses are spread via a usb stick or a shared resource. If we use this spreading method where we have a targeted attack the attacker will have more information about the network.

feit uit security rapport symantec

The attacker can choose at which rate it will drop a virus on one of the nodes on the network. The cost of dropping a virus will be the same. It will not increase. If it will increase this means that the attacker will eventually drop out of the game because it becomes to expensive.
The attacker is in control over the game if it manages to infect a subset of all the resources of the company network.

3.3.2 Actions of the defender

The attacker wants to protect all the nodes of his network. It can do so by getting back control over the resources. We will assume that the defender of the network has knowledge over his own network. Which is convenient in the real world because a company has to know how his infrastructure looks like.

The defender has two possible ways of defending its network:

1. The defender flips all the nodes of his network

2. The defender will flip a subset of the nodes of his network

The cost of flipping all the nods of the network will be greater than the cost of flipping a subset of nodes. We make this assumption because otherwise it will be beneficial for the defender to always flip all the nodes in the network.

We will also make the assumption that as a defender flips a node the node can get infected again. A flip will not be correlated to a patch but to a clean-up. Another setting of the game can be that the flip of the defender is equal to a patch and that the resource cannot be infected any more. But with this case we deviate from the flipIt game, because the attacker cannot flip the resource any more. Unless we work with different virusses every time the attacker flips. We start with the less complex game of flipping is equal to a clean-up.

waarom geen patch, wormen kunnen veranderen gaandeweg

andere mogelijkheid:

3.4 Formal definition Game

In this section we provide a formal definition of the game and the notation that we will use throughout the paper.

Playing periodically with virus propagation

This chapter explains how to model a FlipIt game with a virus propagation that infects a network. The first section explains the difference between a normal FlipIt game and a FlipIt game with virus propagation. The next section derives a formula to calculate the benefit for a FlipIt game with a virus propagation. In the last section we calculate the Nash equilibrium for the benefit formula.

3.5 Benefit for FlipIt game with virus propagation

Periodic Game with delay for the attacker:

Case 1: $\delta_D \leq \delta_A$(The defender plays at least as fast as the attacker.)

Let $r = \dfrac{\delta_D}{\delta_A}$. The intervals between two consecutive defender's moves have length δ_D. Consider a given defender move interval. The probability over the attacker's phase selection that the attacker moves in this interval is r. Given that the attacker moves within the interval, he moves exactly once within the interval (since $\delta_D \leq \delta_A$) and his move is distributed uniformly at random.

The expected period of attacker control within the interval would be r/2, without considering the delay.

However, because of the delay, the maximal time of control is reduced to $\delta_D - d$. There is a probability of r that the attacker will move in the interval of the defender. The attacker has to play soon enough to gain control, meaning that the attacker has to play during the period of $\delta_D - d$ during the interval of the defender. There is $\dfrac{\delta_D - d}{\delta_D}$ probability that the attacker will move soon enough which gives the attacker a gain of $\dfrac{\delta_D - d}{2}$. If the attacker moves after the period of $\delta_D - d$, the gain of the attacker will be zero. The average gain rate of the attacker can be expressed as follows if we look at one interval of the defender:

$$\beta_A(\alpha_D, \alpha_A) = \frac{1}{\delta_D}[\frac{\delta_D}{\delta_A} \cdot \frac{\delta_D - d}{\delta_D} \cdot \frac{\delta_D - d}{2} + \frac{\delta_D}{\delta_A} \cdot \frac{d}{\delta_D} \cdot 0] \tag{3.1}$$

To complete the formula to derive the benefit function, the cost of moving is added. In the second formula we can see the formula of the original FlipIt game.

$$\beta_A(\alpha_D, \alpha_A) = \frac{(\delta_D - d)^2}{2 \cdot \delta_D \delta_A} - k_A \alpha_A \tag{3.2}$$

$$\beta_A(\alpha_D, \alpha_A) = \frac{\delta_D}{2 \cdot \delta_A} - k_A \alpha_A + \frac{d}{\delta_A} + \frac{d^2}{2 \cdot \delta_A \delta_D} \tag{3.3}$$

The benefit of the defender is expressed as follows:

$$\beta_D(\alpha_D, \alpha_A) = 1 - \frac{(\delta_D - d)^2}{2 \cdot \delta_D \delta_A} - k_D \alpha_D \tag{3.4}$$

Case 2: $\delta_A \leq \delta_D$ (The attacker plays at least as fast as the defender.)

Let $r = \dfrac{\delta_D}{\delta_A}$. The intervals between two consecutive attacker's moves have length δ_A. Consider a given attackers move interval. The probability over the attacker's phase selection that the defender moves in this interval is $\dfrac{\delta_D}{\delta_A} = (1/r)$. Given that the defender moves within the interval, he moves exactly once within the interval (since$\delta_A \leq \delta_D$) and his move is distributed uniformly at random.

3.6 something

Periodic Game with delay for the attacker:

Case 1: $\delta_D \leq \delta_A$(The defender plays at least as fast as the attacker.)

Let $r = \dfrac{\delta_D}{\delta_A}$. The intervals between two consecutive defender's moves have length δ_D. Consider a given defender move interval. The probability over the attacker's phase selection that the attacker moves in this interval is r. Given that the attacker moves within the interval, he moves exactly once within the interval (since $\delta_D \leq \delta_A$) and his move is distributed uniformly at random.

The expected period of attacker control within the interval would be r/2, without considering the delay.

However, because of the delay, the maximal time of control is reduced to $\delta_D - d$. If we consider a duration of $\delta_D \cdot \delta_A$ the attacker will play δ_D times. If the attacker plays soon enough it will get a gain of $\dfrac{\delta_D - d}{2}$ in $\delta_D - d$ of the cases. In d cases it will receive a gain of zero. This is the case were the duration of the delay causes the defender to play before the attacker can get control over the resource. So the gain of the attacker can be expressed as follows:

$$Gain = \frac{\delta_D - d}{2} \cdot (\delta_D - d) + 0 \cdot d = \frac{\delta_D - d}{2} \cdot (\delta_D - d) \tag{3.5}$$

The benefit of the attacker can be expressed as follows

$$\beta_A(\alpha_D, \alpha_A) = \frac{(\delta_D - d)^2}{2 \cdot \delta_D \delta_A} + k_A \cdot \alpha_A \tag{3.6}$$

$$\beta_A(\alpha_D, \alpha_A) = \frac{\delta_D}{2 \cdot \delta_A} + k_A \cdot \alpha_A + \frac{d}{\delta_A} + \frac{d^2}{2 \cdot \delta_A \delta_D} \tag{3.7}$$

The benefit of the defender is then:

$$\beta_D(\alpha_D, \alpha_A) = 1 - \frac{(\delta_D - d)^2}{2 \cdot \delta_D \cdot \delta_A} + k_D \cdot \alpha_D \tag{3.8}$$

$$\beta_D(\alpha_D, \alpha_A) = 1 - \frac{\delta_D}{2 \cdot \delta_A} + k_D \cdot \alpha_D - \frac{d}{\delta_A} - \frac{d^2}{2 \cdot \delta_A \delta_D} \tag{3.9}$$

Case 2: $\delta_A \leq \delta_D$ (The attacker plays at least as fast as the defender.)

Let $r = \frac{\delta_D}{\delta_A}$. The intervals between two consecutive attacker's moves have length δ_A. Consider a given attackers move interval. The probability over the attacker's phase selection that the defender moves in this interval is $\frac{\delta_D}{\delta_A} = (1/r)$. Given that the defender moves within the interval, he moves exactly once within the interval (since$\delta_A \leq \delta_D$) and his move is distributed uniformly at random.

If we consider a duration of $\delta_A \cdot \delta_D$ there is a probability of $\frac{\delta_A}{\delta_D}$ that the defender moves within the interval of the attacker. The defender will then receive an average gain of $\frac{\delta_A}{2}$. There is $1 - \frac{\delta_A}{\delta_D}$ probability that the defender will not move in the interval of the attacker and so the defender will receive no gain. The benefit can be expressed as follows when the defender plays δ_D times during a duration of $\delta_A \cdot \delta_D$:

$$\beta_D(\alpha_D, \alpha_A) = \frac{1}{\delta_A \delta_D} \cdot \delta_D \cdot [\frac{\delta_A}{\delta_D} \cdot \frac{\delta_A}{2} + [1 - \frac{\delta_A}{\delta_D}] \cdot 0] + k_D \cdot \alpha_D \tag{3.10}$$

$$\beta_D(\alpha_D, \alpha_A) = \frac{\delta_A}{2 \cdot \delta_D} + k_D \cdot \alpha_D$$

same as the FlipIt solution

(3.11)

However, because of the delay, the maximal time of control of the defender is increased by d. In other words, the defender has some benefit time of d before the attacker really gains control over the resource, meaning that the attacker gains control only after $\delta_A + d$ instead of after δ_A. So, when the defender plays, with a probability of $\frac{\delta_A}{\delta_D}$, the expected gain of the defender's control in this interval would be more than half of the period δ_A: it is $\frac{\delta_A + d}{2}$. There is $1 - \frac{\delta_A}{\delta_D}$ probability that the defender will not move in the interval of the attacker but because of the delay the defender will receive a gain of d. So the benefit of the defender can be expressed as:

$$\beta_D(\alpha_D, \alpha_A) = \frac{1}{\delta_A \delta_D} \cdot \delta_D \cdot [\frac{\delta_A}{\delta_D} \cdot \frac{\delta_A + d}{2} + [1 - \frac{\delta_A}{\delta_D}] \cdot d] + k_D \cdot \alpha_D \tag{3.12}$$

$$\beta_D(\alpha_D, \alpha_A) = \frac{\delta_A - d}{2 \cdot \delta_D} + \frac{d}{\delta_A} + k_D \cdot \alpha_D \tag{3.13}$$

The benefit of the attacker is expressed as follows:

$$\beta_A(\alpha_D, \alpha_A) = 1 - [\frac{\delta_A - d}{2 \cdot \delta_D} + \frac{d}{\delta_A}] + k_A \cdot \alpha_A \tag{3.14}$$

3.7 Simulation

Hoofdstuk 4

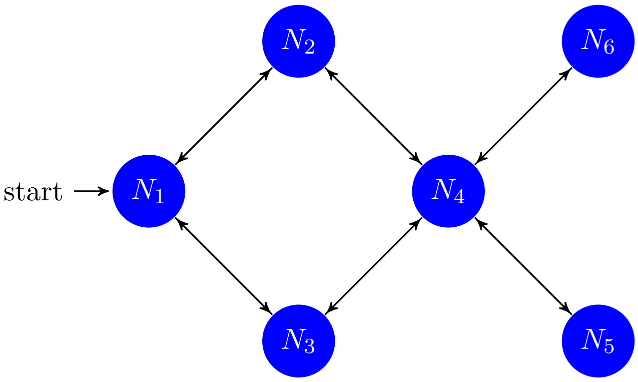
Virus Propagation

4.1 Methods of virus propagation

4.2 REpresenting Virus Propagation in a network

source: http://en.wikipedia.org/wiki/Adjacency_matrix
We model the network through an undirected Graph $G =< V, E >$ where $|V|$ denotes the number of resources in the network and $|E|$ the number of connections. We can convert this to a adjacent matrix where we can represent which vertices of the graph are neighbours of other vertices.
For our graph we have an $|V| \times |V|$ matrix with on every entry a_{ij} a 1 as value if there is a connection between node V_i and V_j and with zeros its diagonal. Because our graph is undirected we have a symmetric matrix.

"If A is the adjacency matrix of the directed or undirected graph G, then the matrix A^n (i.e., the matrix product of n copies of A) has an interesting interpretation: the entry in row i and column j gives the number of (directed or undirected) walks of length n from vertex i to vertex j. If n is the smallest nonnegative integer, such that for all i ,j , the (i,j)-entry of $A^n > 0$, then n is the distance between vertex i and vertex j." [Wikipedia]



The adjacent matrix becomes this matrix $[A]$:

$$\begin{array}{c|cccccc} & N_1 & N_2 & N_3 & N_4 & N_5 & N_6 \\ N_1 & 0 & 1 & 1 & 0 & 0 & 0 \\ N_2 & 1 & 0 & 0 & 1 & 0 & 0 \\ N_3 & 1 & 0 & 0 & 1 & 0 & 0 \\ N_4 & 0 & 1 & 1 & 0 & 1 & 1 \\ N_5 & 0 & 0 & 0 & 1 & 0 & 0 \\ N_6 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}$$

Matrix $A \times A = A^2$ becomes the matrix with the number of paths with 2 steps from N_i to N_j: We denote this matrix as matrix *[B]*

$$\begin{array}{c|cccccc} & N_1 & N_2 & N_3 & N_4 & N_5 & N_6 \\ N_1 & 2 & 0 & 0 & 2 & 0 & 0 \\ N_2 & 0 & 2 & 2 & 0 & 1 & 1 \\ N_3 & 0 & 2 & 2 & 0 & 1 & 1 \\ N_4 & 2 & 0 & 0 & 4 & 0 & 0 \\ N_5 & 0 & 1 & 1 & 0 & 1 & 1 \\ N_6 & 0 & 1 & 1 & 0 & 1 & 1 \end{array}$$

Matrix $A^2 \times A = A^3$ becomes the matrix with the number of paths with 3 steps from N_i to N_j: We denote this matrix as matrix *[C]*

$$\begin{array}{c|cccccc} & N_1 & N_2 & N_3 & N_4 & N_5 & N_6 \\ N_1 & 0 & 4 & 4 & 0 & 2 & 2 \\ N_2 & 4 & 0 & 0 & 6 & 0 & 0 \\ N_3 & 4 & 0 & 0 & 6 & 0 & 0 \\ N_4 & 0 & 6 & 6 & 0 & 4 & 4 \\ N_5 & 2 & 0 & 0 & 4 & 0 & 0 \\ N_6 & 2 & 0 & 0 & 4 & 0 & 0 \end{array}$$

So for A^N every a_{ij} entry gives the number of paths with N steps from N_i to N_j.

With this knowledge we can calculate in how many steps a node is infected. A calculates which nodes are infected after 1 step, A^N calculates which nodes are infected in N steps.. So if we want to know how many nodes are infected after 3 steps we have to add every matrix $(A + A^2 + A^3)$ and see which entry is a non zero entry.

What do we need for an algorithm

Graph network $G =< V, E >$

Graph matrix $[A]$ which is $|V| \times |V|$

Attack vector $[X]$ which is $1 \times |V|$

cummulative matrix $[M]$ which is $|V| \times |V|$

state matrix $[T]$ which is $|V| \times |V|$

Reset vector $[R]$

duration d

time n

rate δ_0 of defender and δ_1 of attacker

Initialisation algorithm:

```
initialisatie
d=0
A=basismatrix
M=A^{0}
n=0
\delta_{0}
\delta_{1}
X
R
controller = defender
```

```
Algorithm
n:= n + 1;
Check who is in control? ( through modulo )
if ( defender & controller=defender)
d:= d + 1;

if ( defender & controller=attacker )
G = X \times R  (flippen ten voordele van defender)
d = 0
controller = defender

if ( attacker & controller=defender )
controller=attacker
..

if ( attacker & contoller=attacker )
d:= d + 1
M = M x A
T = T + M
G = X x T
```

Bijlagen

Bijlage A

The First Appendix

Appendices hold useful data which is not essential to understand the work done in the master thesis. An example is a (program) source. An appendix can also have sections as well as figures and references[**?**].

A.1 More Lorem

Bijlage B

The Last Appendix

Appendices are numbered with letters, but the sections and subsections use arabic numerals, as can be seen below.

B.1 Lorem 20-24

KU Leuven Faculteit Ingenieurswetenschappen 2014 – 2015

Fiche masterproef

Student: Sophie Marien

Titel: Gametheory and Cybersecurity: a study FlipIt and multiple resources

Engelse titel: Beste masterproef ooit al geschreven

UDC: 621.3

Korte inhoud:

Hier komt een heel bondig abstract van hooguit 500 woorden. LaTeX commando's mogen hier gebruikt worden. Blanco lijnen (of het commando `\par`) zijn wel niet toegelaten!

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Thesis voorgedragen tot het behalen van de graad van Master of Science in de ingenieurswetenschappen: computerwetenschappen, hoofdspecialisatie Veilige software

Promotor: Prof. dr. ir. Tom Holvoet

Assessoren: Ir. W. Eetveel
W. Eetrest

Begeleider: Ir. Jonathan Merlevede, Ir. Kristof Coninx