KU LEUVEN

FACULTEIT INGENIEURSWETENSCHAPPEN

Gametheory and Cybersecurity: a study FlipIt and multiple resources

Sophie Marien

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

Todo list

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

Lijst van tabellen

List of Abbreviations and Symbols

Abbreviations

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

Hoofdstuk 1

Introduction

The first contains a general introduction to the work. The goals are defined and the modus operandi is explained.

bib referenties in orde brengen

1.1 Introduction

Security is an important asset in Computer Science. Defending a network of a company is not an easy job. To prevent intruders it can make use of firewalls, routers, IDS systems, virus scans, and other defence mechanisms. Unfortunately technology is growing fast and attacks are getting more sophisticated and the causes of these attacks can be very different. Companies are often the victim of targeted attacks. In a security report of 2014, , states that 80% of the companies are the victims of targeted attacks. Many companies don't see themselves as a target, but sometimes they might be collateral, the target on the way to the real target. This means that everybody can be a target. Corporate networks should continuously defend themselves against outside invaders such as viruses and worms. By doing so the network administrator can keep the network as malware-free as possible. If there is an intruder managed to penetrate the network then the network manager this intruder trying to get out as quickly as possible. This is not always easy. Especially when the intruders secretly sneak and then spread rapidly. In this paper we will work further on the work made by Marten van Dijk, Ari Juels, Alina Oprea and Ronals L. Rivest who wrote a report on the Game FlipIt. FlipIt is a the game of "Stealthy Takeovers". It models a game by means of two players, the attacker and the defender. Both can gain control over a single shared resource by flipping it. The most important property of the game is that the flipping happens stealthy. This means that the players have no clue about when the other player moves. The goal of the game is to maximise the time the player controls the resource minus the average cost of the flipping.

iets tussen nog

verwijzing naar report

verwijzing naar FlipIT

1

1.1.1   Motivation of the game

1.1.2   Contributions and results

1.1.3   Conclusions

The "I love you"virus is an example of a virus that spreads quickly. This virus propagates via mail systems. If someone opens an email with "I love you"virus in annex this virus spreads itself by sending a mail itself to everyone in your contact list. So the virus can multiply rapidly and eventually a business network shut down by the heavy traffic. In this example, there is a need human interaction to spread the virus to do. If no one opens the virus can not spread the mail. Unfortunately, there are viruses that can spread without human interaction. These viruses are referred to as worms. A worm is also a computer program that replicates itself to spread to other computers so. Via a computer network, copies of the worm forwarded without an intermediary is used for. The worm will use vulnerabilities to infect other computers. Most worms are designed to spread out and just try not to make any changes to the systems that they pass. These worms can still inflict damage by increased network traffic they generate. Worms that contain Harm damage a program to install a backdoor or a rootkit on the infected computers. Backdoors and rootkits ensure that future use can be made of the infected computers. The Stuxnetworm is a very famous worm. Initially this worm spread via infected USB sticks and from then it could spread through the Internet to other computers. The purpose of the Stuxnetworm was broken to run the centrifuges in nuclear reactors. Many reactors have been infected. From the standpoint of the defender, it is very important to respond as quickly as possible so that the worm can not spread quickly.

1.2   introduction number 2

(We live in an era) In this era where digitalization becomes prominent in every aspect of our lives, where technology is growing fast and where business are always under attack, security becomes an issue of increasing complexity. Since 2009, the number of reported security attacks has increased 66%, year over year. . These numbers only represent the attacks that are detected. In 2014 117,339 attacks where coming in daily. Many of those attacks have a different cause. Some of them can be benign, others can be harmful. Many companies are unaware of all the attacks. Some of them think that they are not a target, but they might be a target on the way to a real target. Recently there where some high profiled targeted attacks which have been revealed. (Belgacom). Targeted attacks are ... The *Kill Chain* is a concept by Lockheed Martin Corporation, explained in the whitepaper . It explains the different phases of a typical attack from the view of an attacker. It also outlines the typical attacker activities on the right. This model is very useful to define the different moments of the life cycle of an attack and when a company should act to defend itself. In this paper we would like to prevent the viruses of spreading into the network system of a company. This means that we have to act in phase Installation, Command and Control and Action on Objectives of the kill chain.

[security report van pwc]

[withepaper toevoegen]

Security is an important asset in Computer Science. Defending a network of a company is not an easy job. Malicious people will try to To prevent intruders it can make use of firewalls, routers, IDS systems, virus scans, and other defence mechanisms. Unfortunately technology is growing fast and attacks are getting more sophisticated and the causes of these attacks can be very different. Companies are often the victim of targeted attacks. In a security report of 2014, , states that 80% of the companies are the victims of targeted attacks. Many companies don't see themselves as a target, but sometimes they might be collateral, the target on the way to the real target. This means that everybody can be a target. Corporate networks should continuously defend themselves against outside invaders and targeted attacks. Researchers have already investigated the situations through the FlipIt game in which a system is continuously compromised by an attacker through targeted attacks. FlipIt is a the game of " Stealthy Takeovers". It models a game by means of two players, the attacker and the defender. Both can gain control over a single shared resource by flipping it. The most important property of the game is that the flipping happens stealthy. This means that the players have no clue about when the other player moves and has control over the shared resource. The goal of the game is to maximise the time the player controls the resource minus the average cost of the number of flipping. In this paper we model a company network through multiple shared resources and a flip from the attacker that drops a virus that will spread itself autonomously. We show that ...

iets tussen nog

verwijzing naar report

3

Hoofdstuk 2

FlipIt with virus propagation

2.1 FlipIt vs FlipIt with virus propagation

This chapter explains how to model a FlipIt game with a virus that propagates and infects the nodes in a network. First, this section explains the difference between FlipIt with and without a virus. Then, section 2.2 derives the formula to calculate the gain for a FlipIt game without a virus. After that section 2.3 introduces a modification to this formula to achieve an adapted gain formula for a FlipIt game with virus propagation. This allows us to derive the benefit formula.

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.

`check reff`

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.

2.2   Gain formula for a FlipIt game without virus propagation

In their FlipIt paper [], Marten van Dijk et al. , give a definition of the gain of a player i . This definition is however, in the best of our knowledge, not easy to adapt to the situation with virus propagation. Therefore, this section presents an alternative formula that defines a game by quantifying the amount of time each player has control.

The following notations will be used throughout the formal definition (see figure 2.1 for a graphic representation of some of the notations):

δ_D: This is the period of the defender. This denotes the length of the interval between two consecutive moves of the defender ($\delta_D > 0$).

δ_A: This is the period of the attacker. This denotes the length of the interval between two consecutive moves of the attacker ($\delta_A > 0$).

T_D: This denotes the phase of the defender that was chosen randomly and uniformly over the interval $[0,\delta_D]$.

T_A: This denotes the phase of the attacker that was chosen randomly and uniformly over the interval $[0,\delta_A]$.

Unit of control: Defined as the period between gaining (full) control and losing control over the resource.

n_D: The n'th interval of the defender, starting from interval 0.

n_A: The n'th interval of the attacker, starting from interval 0.

$\Delta Unit_D(n)$: This is a function that denotes the length of a unit of control of the defender in the n'th interval of the attacker or the defender depending on who is playing faster.

$\Delta Unit_A(n)$: This is a function that denotes the length of a unit of control of the attacker in the n'th interval of the attacker or the defender depending on who is playing faster.

lcm(a,b): The least common multiple of a and b.

*gcd(a,b)*: The greatest common divider of a and b.

$G_i(t)$: Gain of player i at time t. The gain of a player is defined as the total amount of time that a player has owned the resource since the start of the game up to time t. In the context of a FlipIt game with virus propagation, the whole network is seen as one resource. This resource is owned by the attacker if he has control over the entire network.

Average Gain: $\gamma_i(t) = G_i(t)/t$ is the average gain rate of player i which is defined as the fraction of time that player i has control over the resource up to time t.

Benefit: The average benefit of a player i is denoted by $\beta_i(t) = \gamma_i(t) - k_i/\delta_i$, which is equal to the fraction of time that the resource has been owned by player i, minus the cost rate for moving. For now we consider the cost rate equal to 0. In the rest of the paper the 'benefit' of the game for player i will be used as shorthand for 'average benefit'.

FIGUUR 2.1: Graphic representation of some of the notations
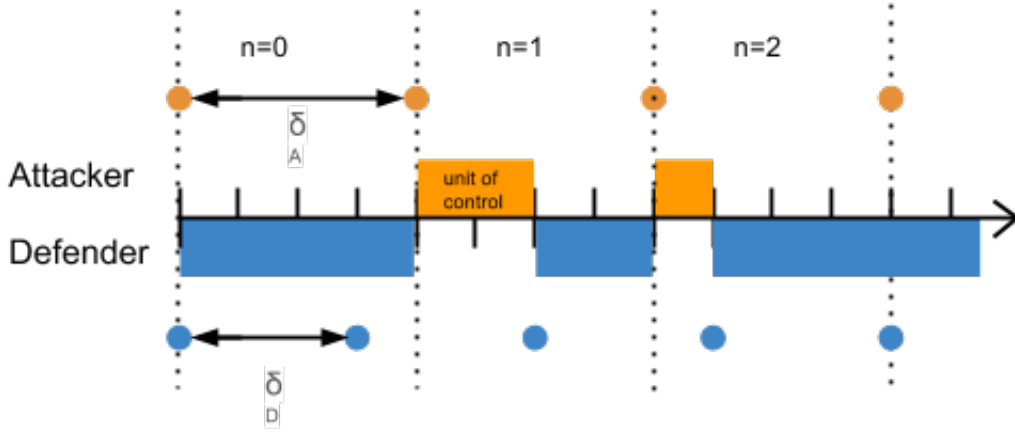
To compute the gain of a player in a periodic game without phases, two cases are considered: case 1 where the defender moves at least as fast as the attacker and case 2 where the attacker plays at least as fast as the defender. Next, the formula is enriched by introducing the phases.

Computing the gain for an attacker of a normal FlipIt game

Consider a game without phases, so in which both players start with a phase T_D and phase T_A equal to zero. Both players start their first move at $t = 0$. As previously stated (in the formal definition of the game and the introduction of different notations used throughout the paper), the defender has control in the beginning of the game at $t = 0$. For the remainder of the game, if the two players move at the same time during the game, the moves cancel each other out and no change of state happens.

Case 1:

$\delta_A \geq \delta_D$ (The defender moves at least as fast as the attacker.)

To compute the gain formula for the attacker,the amount of time that the attacker has control over the resource from the start of the game up to time t has to be calculated. This can be done by computing the sum of all the units of control of the attacker up to time t.

To calculate a single unit of control of the attacker, the time line of the FlipIt game is divided into intervals of size δ_A. Every time the attacker moves we have the start of a new interval, with the attacker being in control, unless there is a simultaneous move with the defender. Considering that the defender moves at least as fast as the attacker, he or she will at least move one time during the interval of the attacker. Because the attacker only moves at the start of his or her interval we can say that the defender will always end as being in control of the resource at the end of an attacker's interval. .
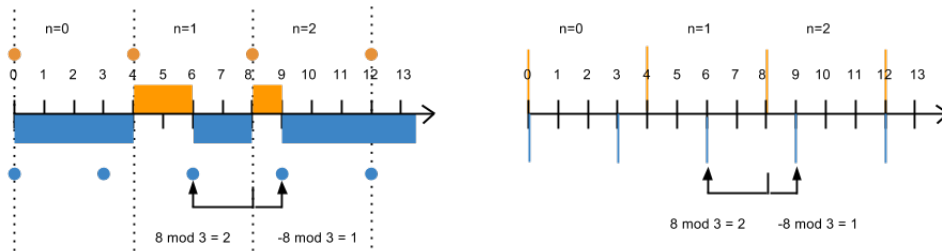
To calculate how long the unit of control of the attacker is in the n'th interval, we only need to know how long the attacker has control over the resource before the defender moves in that interval. The start time of the n'th interval will be a multiple of the period of the attacker. Once the attacker has played, the time he can stay in control until the next move of the defender, depends on the time elapsed since the last time the defender played in the previous interval (the (n-1)th interval).

The time at which the defender plays in an interval is a multiple of its period. Once the defender has played for the last time in the (n-1)'th interval, the remaining time until the attacker will play can be calculated as $n \cdot \delta_a$ *modulo* δ_D which is equal to the remainder of $n \cdot \delta_A$ divided by δ_D. [referentie naar matworks: $http://nl.mathworks.com/help/matlab/ref/mod.html$]The time the attacker will stay in control is then $\delta_D - n \cdot \delta_A$ *modulo* δ_D, which can also be calculated as $(-n \cdot \delta_A)$ *modulo* δ_D.

Figure 2.2 illustrates this graphically, for $\delta_A = 4$, $\delta_D = 3$ and the $n = 2$ interval. We see that in interval 1, the defender will stay 8 *modulo* $3 = 2$ in control, and so, in interval 2, the attacker will stay $1 = 3 - 2 = -(2 * 4)$ *modulo* 3 in control.

FIGUUR 2.2: Taking the modulo of a negative number

This brings us to the next formula to calculate the length of a unit of control in the n'th interval of the attacker.

For every positive and non zero real δ_A and $\delta_D \in \mathbb{R}$ and every $n \in \mathbb{N}$ (including 0 in the set of natural numbers) :

$$\Delta Unit_A(n_A) = [(-n_A) \cdot \delta_A] mod \delta_D \tag{2.1}$$

where n_A is the number of the n'th interval of the attacker starting from interval 0 where the length of the unit of control of the attacker is calculated.

The length of a unit of control of the defender is the remainder of the interval after the attacker loses control over the resource when the defender plays. This can be defines as follows for the n'th interval of the attacker:

$$\Delta Unit_D(n_A) = \delta_A - [(-n_A) \cdot \delta_A] mod \delta_D \tag{2.2}$$

An example: Figure 2.2 shows a FlipIt game were the period of the attacker is π and the period of the defender is 1. ... On figure 2.3 $\boxed{\text{aanvullen}}$

FIGUUR 2.3: Example for calculating the control unit in interval 3 for a FlipIt game with period defender = 1 and period attacker = pi
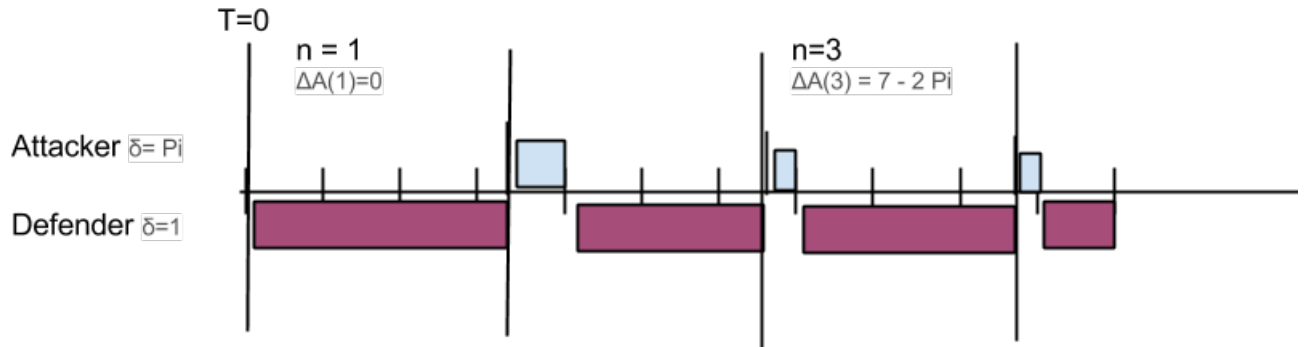
The gain formula can be calculated by taking all the units of control of the player up to an amount of p intervals of the attacker. The gain formula for the attacker is stated as follows:

$$Gain_A = \sum_{i=0}^{p} \{[(-i) \cdot \delta_A] mod \delta_D\}\} \tag{2.3}$$

where p is the number of units of control that have to be summed.

The gain of the defender is the sum of the units of control of the defender up to the same amount of p intervals of the attacker:

$$Gain_D = \sum_{i=0}^{p} \{\delta_A - [(-i) \cdot \delta_A] mod \delta_D\}\} \tag{2.4}$$

9

$$Gain_D = \sum_{i=0}^{p}\{\delta_A \cdot i\} - \sum_{i=0}^{p}\{[(-i) \cdot \delta_A]mod\delta_D\}\} \tag{2.5}$$

$$Gain_D = \delta_A \cdot p - \sum_{i=0}^{p}\{[(-i) \cdot \delta_A]mod\delta_D\}\} \tag{2.6}$$

Note: The gain formula is not in function of time t but the amount of p intervals of the attacker. This approach is chosen because it will result in whole units of control. It is possible to make a gain formula using the time, but this will result in a much more complicated function.

For phases ..

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

For this case we use the same approach as in case 1 but with a small difference. To compute the unit of control of both players we divide the time line of the FlipIt game into intervals of size δ_D. The defender moves at the start of each interval, the end of the interval is the beginning of the next interval. Considering that the attacker will move at least as fast as the defender, he or she will move at least one time during the interval of the defender. Because the defender only moves in the beginning of each interval, the attacker will end as being in control of the resource.

If the unit of control of the defender need to be calculated, we only need to know how long it takes for the attacker to move in the interval. This can be done in the same way as in case 1 by taking the modulo of the negative of the beginning of the interval. The big difference with case 1 is when the length of the unit of control in the 0'th interval is calculated. Because the defender always has control in the beginning of the game, the first interval is computed in a different way. The unit of control of the defender in the 0'th interval is equal to the length of the period of the attacker, since from that moment the attacker takes control.

For every positive and non zero real δ_A and $\delta_D \in \mathbb{R}$ and every $n \in \mathbb{N}$ (including 0 in the set of natural numbers) :

for $n_A = 0$

$$\Delta Unit_D(n_D) = \delta_A \tag{2.7}$$

for $n_A > 0$

$$\Delta Unit_D(n_D) = [(-n_D) \cdot \delta_D]mod\delta_A \tag{2.8}$$

where n_D is the number of the n'th interval of the defender starting form interval 0 where the length of the unit of control of the defender is calculated.

The length of a unit of control of the attacker is the remainder of the interval after the defender loses control over the resource when the attacker plays. This can be defined as follows for the n'th interval of the defender:

$$\Delta Unit_A(n_D) = \delta_D - \Delta Unit_D(n_D) \tag{2.9}$$

The gain formula for $\delta_D \geq \delta_A$ is calculated in the same manner as case 1:

The gain of the defender is the sum of the units of control of the defender up to the same amount of p intervals of the attacker:

$$Gain_D = \sum_{i=1}^{p} \{[(-i) \cdot \delta_D] mod \delta_A\} \ \ with \ \ i = 0 \ \ Gain_D = \delta_A \qquad (2.10)$$

and for the attacker:

$$Gain_A = \delta_D \cdot p - \sum_{i=1}^{p} \{[(-i) \cdot \delta_D] mod \delta_A\} \ \ with \ \ i = 0 \ \ Gain_A = \delta_D - \delta_A \quad (2.11)$$

2.3 Gain and benefit formula for a FlipIt game with virus propagation

The formulas from the previous section can now be adapted to calculate the gain of both players in a FlipIt game with virus propagation. As mentioned before, the attacker will try to infect all the nodes in the network. He 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. 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 explained in section [matrix berekeningen]. 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.

The previous section defined a formula to calculate each unit of control of the attacker and the defender for two cases. If the virus propagation takes *d* time before every resource is infected then this *d* has to be subtracted from each unit of control. (see figure 7.4 2.4). It may happen that the unit of control is less than *d*. In that case, the result of the substration will be a negative number, meaning that the defender has flipped all the resources before the attacker could gain control over all the resources. To calculate the gain only the units of control bigger than 0 have to be summed. So the formula becomes:

For $\delta_A \geq \delta_D$:

$$Gain_A = \sum_{i=0}^{p} \{[(-i) \cdot \delta_A] mod \delta_D - d\} > 0\} \qquad (2.12)$$

where p is the number of units of control that have to be summed.

The gain of the defender is equal to the amount of time that the attacker is not in control of the resource. So the formula for the defender becomes:

$$Gain_D = p \cdot \delta_A - \sum_{i=0}^{p}\{[(-i) \cdot \delta_A]mod\delta_D - d\} > 0\} \qquad (2.13)$$

For $\delta_D \geq \delta_A$:

$$Gain_A = \delta_D \cdot p - \sum_{i=1}^{p}\{[(-i) \cdot \delta_D]mod\delta_A - d\} > 0\} \qquad (2.14a)$$

$$with \quad i = 0 \quad Gain_A = \delta_D - (\delta_A - d) > 0 \qquad (2.14b)$$

$$(2.14c)$$
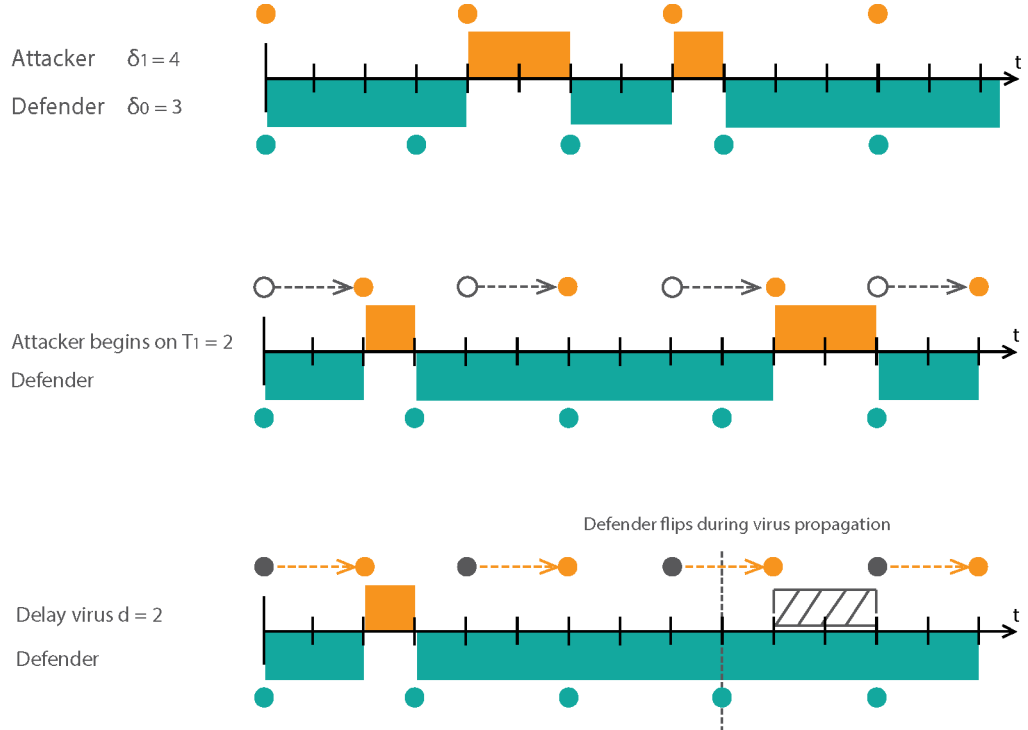
and for the defender:

$$Gain_D = \sum_{i=1}^{p}\{[(-i) \cdot \delta_D]mod\delta_A - d\} > 0\} \qquad (2.15a)$$

$$with \quad i = 0 \quad Gain_D = \delta_A - d > 0 \qquad (2.15b)$$

$$(2.15c)$$

FIGUUR 2.4: Difference in a FlipIt game between delay caused by a virus and a phase bigger than zero for the Attacker

Computing the benefit of a FlipIt game with virus propagation

Calculating the benefit of both players, requires calculating the average gain rate of both players. To compute the benefit the value of parameter p needs to be determined. Two cases can be considered: one case where δ_D and $\delta_A \in \mathbb{Q}$ and the other one where δ_D and $\delta_A \in \mathbb{I}$. In both cases we first calculate the benefit of the attacker in case that the defender moves at least as fast as the attacker. The benefit of the defender will be BenD = 1 - BenA. The benefit of both players for the case where the defender moves as least as fast as the defender is done in a similar way.

Rational numbers ($\mathbb{Q}$): When δ_D and δ_A are rational numbers, after a number of intervals (namely their least common multiple), the same pattern of intervals will be repeated over and over again. Why? A rational number is a number that can be expressed as the fraction p/q with p and q $\in \mathbb{Z}$ (integers), with the denominator q not equal to zero, it is possible to find the *lcm* of δ_D and δ_A. The *lcm* is defined for all rational numbers as: $lcm(\frac{a}{b}, \frac{c}{d}) = \frac{lcm(a,c)}{gcd(b,d)} with$ []. When t is equal to the [referentie] *lcm* of δ_D and δ_A, both players will move again at the same time and this can be mapped to the beginning of the game. Because we stated that at the end of the interval of the attacker, the defender is in control and because if two players move at the same time the moves cancel each other out, we can map this to the beginning of the game. Since the game goes on infinitely, to calculate the average gain of the attacker, it is sufficient to calculate the average gain of the attacker only during a period of time equal to the *lcm* of δ_D and δ_A. Since *lcm* is a multiple of δ_D and δ_A, there is a number p so that *lcm* =p $\cdot \delta_A$, meaning that the attacker will have played p times. p can be defined as follows:

$$p = \frac{lcm(\delta_D, \delta_A)}{\delta_A} \tag{2.16}$$

This results in the following formula for the benefit of the attacker with a cost rate equal to zero:

$$\beta_A = \frac{\sum_{i=0}^{p}[[(-i) \cdot \delta_A]mod\delta_D - d] > 0}{lcm(\delta_D, \delta_A)} \tag{2.17}$$

As stated before [], the benefit of the attacker and the benefit of the defender add up to 1 ($\beta_A + \beta_B = 1$). The benefit of the defender can be writen as follows:

$$\beta_D = 1 - \beta_A \tag{2.18}$$

Irrational numbers ($\mathbb{I}$): If δ_D and/or $\delta_A \in \mathbb{I}$: An irrational number $i \neq \frac{a}{b}$ with $b \in \mathbb{Z}$, a $\in \mathbb{N}$.

Two cases can be distinguished. (A) $\frac{\delta_D}{\delta_A}$ is a rational number a/b with a $<=$ b. In that case, after b intervals, the pattern will repeat itself.

(B)If either δ_D and δ_A cannot be written as a fraction, and they are no multiple of each other, the least common multiplier cannot be calculated. Moreover, there

will be no repeating pattern. If both players move at one point in the game at the same moment, this point of time has to be a multiple of the period of the attacker and a multiple of the period of the defender. But because there is no least common multiple, no such point of time exists during the game. If both players never play at the same moment, it is not possible to have a repeated pattern because no mapping to the beginning of the game can occur. Additionally two unit of controls with the same length cannot exist. This would mean that the game has a repeated pattern, which is not possible.

The game will go on forever, if no repeating pattern occurs and it would keep on generating units of control with different lengths. This implies that if the game goes on forever, every length between 0 and the smallest interval (which is δ_D) will be generated. To calculate the benefit we want to summarize the unit of controls up to a number of interval p. Considering that the game goes on forever without repetition we cannot rely on the fact that the benefit can also be calculated only during the repetition. Calculating the benefit of a game without repetition would imply that all the unit of control to infinite have to be calculated. This implicates that all the numbers between 0 and δ_D have to be summed but this is impossible. *The reals are uncountable; that is: while both the set of all natural numbers and the set of all real numbers are infinite sets, there can be no one-to-one function from the real numbers to the natural numbers* [WikiPedia: real numbers] If they are uncountable that means that we cannot calculate the sum of all the numbers between 0 and the biggest interval. This is proved by the Cantor diagonalisation argument. Uncountable does not mean that we cannot order it. The Field of the real numbers is ordered.

nog mooie tekst schrijven in engels: hier essentie

We kunnen de benefit wel benaderen door een zo groot mogelijke som te nemen van de unit of controls. Uit deze benadering is af te leiden waar de verhouding naartoe zou gaan als de limiet zou genomen worden. -> laten zien met een voorbeeld van Pi en 1.

Hoofdstuk 3

Formula

3.1   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:

$$Gain = \frac{\delta_D - d}{2} \cdot (\delta_D - d) + 0 \cdot d = \frac{\delta_D - d}{2} \cdot (\delta_D - d) \tag{3.1}$$

The benefit of the attacker can be expressed as follows

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

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

The benefit of the defender is then:

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

$$\beta_D(\alpha_D, \alpha_A) = 1 - \frac{\delta_D}{2 \cdot \delta_A} + k_D \cdot \alpha_D - \frac{d}{\delta_A} - \frac{d^2}{2 \cdot \delta_A \delta_D} \tag{3.5}$$

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 $\delta_A \cdot \delta_D$:

$$\beta_D(\alpha_D, \alpha_A) = \frac{1}{\delta_A \delta_D} \cdot \delta_D \cdot [\frac{\delta_A}{\delta_D} \cdot \frac{\delta_A}{2} + [1 - \frac{\delta_A}{\delta_D}] \cdot 0] + k_D \cdot \alpha_D \tag{3.6}$$

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

same as the FlipIt solution

$$\tag{3.7}$$

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:

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

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

The benefit of the attacker is expressed as follows:

$$\beta_A(\alpha_D, \alpha_A) = 1 - [\frac{\delta_A - d}{2 \cdot \delta_D} + \frac{d}{\delta_A}] + k_A \cdot \alpha_A \qquad (3.10)$$

Hoofdstuk 4

The Final Chapter

4.1   chap

Hoofdstuk 5

Conclusion

The final chapter contains the overall conclusion. It also contains suggestions for future work and industrial applications.

5.1 trala

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

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