KU LEUVEN

FACULTEIT INGENIEURSWETENSCHAPPEN

Flip the virus: Modelling targeted attacks using FlipIt with propagation delay

Sophie Marien

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

Promotor:
Prof. dr. T. Holvoet

Assessoren:
Prof. dr. B. Jacobs
Dr. ir. A. Dries

Begeleiders:
Ir. Jonathan Merlevede,
Ir. Kristof Coninx

Academiejaar 2014 – 2015

Voorwoord

Many people have helped in the realization of this thesis. I would like to thank everybody who kept me busy the last year and made it possible for me to finish my thesis.

First I would like to thank my promoter and my assistants for their excellent support during the writing of this paper. They helped me figure out what to do and put a lot of time and effort in me.

Second I would like to thank my parents for their patient with me. A special thanks goes to my mother, who helped me a lot with my thesis and told me how to write in a structured way. Without her this thesis would be incomprehensible. Also a thank for my brother for his insights into mathematics that gave me a different angle to look at problems.

I would also like to thank my boyfriend who supported me during the writing of this thesis and helped me to write a beautiful text.

Last but not least all the people that read my thesis for faults: ..
A few other people earn a special mention: Revue-blokt for keeping me focused on my thesis, DistriNet labo for letting me in and study in a quit place, Antonio for distracting me and telling me stories about his travels. A special memorial to John Nash, a mathematician with a fundamental contribution to Game Theory, that died in a car accident during the writing of this thesis. His Nash Equilibrium is used in this thesis..

Sophie Marien

Inhoudsopgave

Voorwoord **i**

Samenvatting **iv**

Samenvatting **v**

Lijst van figuren en tabellen **ix**

1 Introduction **1**
1.1 Introduction 1

2 Intoduction to GameTheory **5**
2.1 What is cyber security? 5
2.2 Intro game theory 8
2.3 A brief introduction in Game Theory 8
2.4 The FlipIt game 10
2.5 Extensions on FlipIt 12

3 FlipIt game with virus propagation **15**
3.1 Introduction 15
3.2 FlipIt game with virus propagation 15
3.3 Explaining difference between FlipIt with and without virus propagation 15
3.4 Playing periodically with virus propagation 16

4 Nash Equilibria **23**
4.1 Nash Equilibria 23

5 Conclusion **29**
5.1 trala 29

Bibliografie **31**

Todo list

Results toevoegen iv
laatset zinnen niet correct vii
misschien meer zeggen over APTs en threats 1
tekst overgenomen van wikipedia 6
toevoegen referentie naar kaspersky APT report 7
site kaspersky apt 7
APT report 8
optimal strategy uitleggen 9
beter verwoorden 13
dat laatste nog eens nakijken 26

Samenvatting

Recently, high profile targeted attacks such as the attack on Belgacom [2] (a major Belgian telcom), have demonstrated that even the most secure companies can still be compromised, and that moreover such attacks can go undetected for a while. These kind of attacks are called APT, advanced persistent threats, which are designed to penetrate secretly a computer network, collect sensitive data and stay hidden for many years. A company has every interest to mitigate the risks of an APT and the consequences that it can cause. Fighting against these attacks requires methods that go beyond the standard tools against malware. Because of the stealthyness it is better to prevent the attack than detection and recover after it has done some damage.
A group of researchers at the RSA, van Dijk et al., proposed the game FlipIt (The game of "stealthy takeover") to model stealthy takeovers. It is a 2-players game composed of a single attacker, a single defender and a single shared resource. The players will compete to get control over the shared resource. Every move of the players will involve a cost and these moves happen in a stealthy way. The objective of the game for each player is to maximise the fraction of time of controlling the resource and minimise the total move cost.
FlipIt does however not take into account that a move may not be instantaneous, but has a certain delay. In this paper, we restrict ourselves to games where both the defender and the attacker play with a periodic strategy. We adapt FlipIt such that we can use it to model the game of defending a company network that is attacked by a virus. The FlipIt formulas are adapted such as to take the delay for virus propagation into account. The goal of this thesis is to find out if their are interesting Nash Equilibria for a game with a virus propagation delay and if we can learn some lessons out of it.

Results toevoegen

Keywords: Game theory, Advanced persistant threats, cyber security, FlipIt, stealthy takeovers.

Samenvatting

Onlangs zijn er gerichte security aanvallen geweest op grote bedrijven, zoals de aanval op Belgacom (een grote Belgische telcom). Deze aanvallen hebben aangetoond dat zelfs de meest veilige bedrijven nog steeds gecompromitteerd kunnen worden, en dat bovendien dergelijke aanvallen onopgemerkt kunnen blijven voor een bepaalde tijd. Flipit is een model dat door onderzoekers van de RSA (van Dijk et al.) is voorgesteld om dergelijke aanvallen te modelleren. Het is een 2-spelers spel bestaande uit een aanvaller, een verdediger en een gedeelde bron. De spelers proberen om controle te krijgen over de gedeelde bron en ze doen dit op een heimelijke manier. Met FlipIt wordt echter geen rekening mee gehouden dat een aanval niet onmiddellijk is, maar dat dit kan gebeuren met een zekere vertraging. In dit artikel passen we het model van FlipIt zodanig aan dat we het kunnen gebruiken voor heimelijke aanvallen die onderheven zijn aan een vertraging. Resultaat :

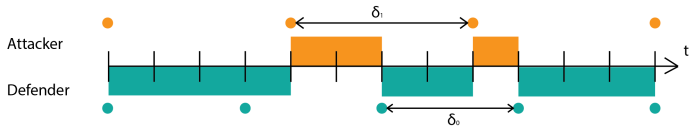
Flipit is een spel geïntroduceerd door Van Dijk et al. Om te begrijpen hoe we het FlipIt spel kunnen aanpassen om virus propagatie in acht te nemen, is het belangrijk om vertrouwd te raken met de concepten van het basische Flipit spel en de notaties. Daarom beginnen we eerst met een uitleg hoe het basische FlipIt spel werkt en de belangrijkste formules die we in de paper gebruiken.

Flipit is een spel met twee spelers met een gedeelde bron die de spelers zo lang mogelijk willen beheren. De gedeelde bron kan een wachtwoord, een netwerk of een geheime sleutel zijn afhankelijk van welke situatie gemodelleerd wordt. In de rest van de paper noemen we de twee spelers de aanvaller, aangegeven met onderschrift A en de verdediger, aangegeven met onderschrift D.

Het spel begint op tijdstip $t = 0$ en blijft voor onbepaalde tijd doorgaan ($t \to \infty$). De tijd van het spel wordt aangenomen als continu. Om controle over de bron te krijgen kunnen de spelers i, met $i \in \{A, D\}$ de bron flippen. Elke flip impliceert een zekere kost k_i en deze kosten kunnen variëren voor elke speler. Beide spelers proberen om hun kosten te minimaliseren. Door een kost in te voeren, voorkomt men dat de spelers te vaak bewegen.

De unieke eigenschap van Flipit is dat elke flip gebeurt op een heimelijke manier, wat betekent dat de speler heeft geen idee dat de andere speler (zijn tegenstander) de bron heeft geflipt. Zo zal de verdediger niet kunnen achterhalen of de bron al is gefipt door de aanvaller tot hij de bron zelf flipt. Het doel van de speler is om zo lang mogelijk de controle te behouden over de bron en terwijl de kost minimaliseren.

Een beweging kan ook leiden tot een "verloren beweging", genoemd een flop. Het kan gebeuren dat de bron reeds onder controle is van de speler. Als de speler flipt wanneer hij of zij al de controle heeft over de bron, dan verspilt de speler een zet omdat het niet leidt tot een verandering van controle en dus een kost verspilt wordt.



Figuur 1: Een afbeelding van een Flipit spel met discrete tijdsintervallen waarbij beide spelers periodiek spelen. Elke beweging of flip wordt aangegeven met een blauw of oranje cirkel. De aanvaller is vertegenwoordigd in het oranje en speelt met een periode van $\delta_A = 4$. De verdediger is vertegenwoordigd in het blauw en speelt met een periode van $\delta_D = 3$. De blauwe en oranje rechthoeken geven de hoeveelheid tijd die de betreffende speler in de controle is van de bron.

De staat van de bron wordt aangeduid als een tijdsafhankelijke variabele $C = C_i(t)$. $C_D(t)$ 1 is als het spel onder controle is van de verdediger en 0 als het spel onder controle is van de aanvaller. Omgekeerd, zal $C_A(t)$ 1 zijn als het spel onder controle is van de aanvaller en 0 als onder controle van de verdediger. Dus, $C_A(t) = 1 - C_D(t)$. Het spel begint met de verdediger in controle: $C_D(0) = 1$.

De spelers krijgen een benefit gelijk aan de hoeveelheid tijd dat ze in het bezit zijn van de bron min de kosten voor het maken van de bewegingen. De kosten van een speler i worden aangegeven met k_i. De totale winst van de speler i is gelijk aan de totale hoeveelheid tijd waarbij een speler i in controle is can de bron vanaf het begin van het spel tot de huidige tijd t. Dit wordt als volgt uitgedrukt:

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

De totale winst van de verdediger opgeteld bij de totale winst van de aanvaller telt op tot t:

$$G_D(t) + G_A(t) = t \tag{2}$$

De gemiddelde winst van speler i wordt gedefinieerd als volgt:

$$\gamma_i(t) = G_i(t)/t. \tag{3}$$

En daarmee voor alle $t > 0$:

$$\gamma_D(t) + \gamma_A(t) = 1 \tag{4}$$

Laat $\beta_i(t)$ is de gemiddelde benefit van een speler i tot aan tijd t:

$$\beta_i(t) = \gamma_i(t) - k_i\alpha_i. \tag{5}$$

Dit is gelijk aan de fractie van de tijd waarbij de bron in handen is van speler i, minus de kosten van het maken van de bewegingen. α_i definieert het gemiddeld aantal flippen door speler i tot tijd t. De asymptotische benefit ratio wordt gedefinieerd als lim inf van de gemiddelde benefit omdat de tijd t toeneemt tot oneindig en de gemiddelde benefit niet beperkend waarden.

$$\beta_i(t) = \lim_{t\to\infty} inf\beta_i(t) \tag{6}$$

laatset zinnen niet correct

strategieën

Omdat de spelers bewegen in een sluipende manier, zijn er verschillende soorten feedback die een speler kan krijgen tijdens het rijden. Dergelijke feedback kan worden verdeeld in twee groepen van strategieën. De niet-adaptieve strategieën en de adaptieve strategieën. Deze worden beschreven in de tabel 1.

Als er geen feedback voor geen van beide spelers, hebben wij een niet-adaptieve strategie. Omdat een speler geen feedback tijdens het spel zal hij spelen op dezelfde manier tegen elke tegenstander. De strategie die niet-adaptieve omdat de speelstrategie niet afhankelijk is van de tegenstander bewegingen. Een interessante subklasse van de niet-adaptieve strategieën die waar de tijdsintervallen tussen twee opeenvolgende bewegingen worden gegenereerd door een vernieuwingsproces. Een voorbeeld hiervan werd strategie is de periodieke strategie waarbij het tijdsverloop tussen twee opeenvolgende bewegingen van de spelers een vast interval. Een exponentiële strategie is vernieuwingsstrategie waarbij het interval tussen twee opeenvolgende zetten exponentieel verdeeld.
In het geval dat er feedback, een speler kan zijn strategie aanpassen aan de ontvangen over de bewegingen van de tegenstander informatie. Afhankelijk van de hoeveelheid informatie ontvangen, kunnen twee subklassen van adaptieve strategieën worden geïdentificeerd. The Last Move (LM) strategieën vertegenwoordigen de klasse waarin wanneer een speler flips zal hij vinden van de exacte tijd dat de tegenstander speelde de laatste keer. In de tweede klasse, genaamd Full History (FH), wanneer een speler flips zal hij vinden van de hele geschiedenis van de beweging van de tegenstander.
In dit artikel zullen we ons richten op de niet-adaptieve strategieën. Deze keuze is ingegeven door het feit dat in een zekerheid spel een speler (verdediger of aanvaller) zelden informatie over de bewegingen (laatste zet of volledige geschiedenis) van zijn tegenstander.

Het onderzoek van de verschillende strategieën middels Flipit framework stelt een aantal interessante resultaten leiden:

- periodieke spellen domineren de andere vernieuwing strategieën, wat betekent dat het altijd voordelig om periodiek tegen een tegenstander met een vernieuwing van de strategie te spelen;

Categories	**Klassen Strategies**
Non-adaptieve (NA)	Vernieuwing
	- Periodieke
	- Exponentiële
	General non-adaptieve
Adaptive (AD)	Laatste move (LM)
	Full History (FH)

Tabel 1: hiërarchie van de klassen van de strategieën in Flipit

- periodieke games zijn nadelig tegen spelers na een laatste zet adaptieve strategie;
- als de verdediger speelt met een periodieke tarief dat snel genoeg is zal hij de aanvaller te dwingen uit te vallen;
-

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.

Dit is het kort geschreven.
Eigenlijk paper in het nederlands schrijven
Intro – positionering – vraagstelling – oplossingen en contributies
Flipit en cybersecurity
Flipit met delay
Berekeningen
Niet zo lang geleden werden APT's ontdekt. (Introzin moet beter en anders). Bedrijven worden door APTs aangevallen. Belangrijk om APTs tegen te gaan. Geven een grote kost aan de bedrijven. Hun stealthy aspect is vervelend en moeilijk aan te pakken. Preventie is beter dan detectie. Eens ze binnen zijn kunnen we veel schade veroorzaken. Conventionele middelen zoals firewalls, malware detection helpen hier niet tegen. Nieuwe methode nodig. Gametheory FlipIt. FlipIt uitleggen. Deze formules gaan we dan omvormen tot ze wel propagatie delay kunnen modelleren. Hiervan berekenen we ook het Nash equilibrium.

Lijst van figuren en tabellen

Lijst van figuren

1 Een afbeelding van een Flipit spel met discrete tijdsintervallen waarbij beide spelers periodiek spelen. Elke beweging of flip wordt aangegeven met een blauw of oranje cirkel. De aanvaller is vertegenwoordigd in het oranje en speelt met een periode van $\delta_A = 4$. De verdediger is vertegenwoordigd in het blauw en speelt met een periode van $\delta_D = 3$. De blauwe en oranje rechthoeken geven de hoeveelheid tijd die de betreffende speler in de controle is van de bron. vi

2.1 A representation of a FlipIt game where both players are playing periodically and at discrete time intervals. Every move or flip is indicated by a blue or orange circle. The attacker is represented in orange and plays with a period of $\delta_A = 4$. The defender is represented in blue and plays with a period of $\delta_D = 3$. The blue and orange rectangles represent the amount of time the respective player is in control of the resource. . . 10

3.1 Formalization of a FlipIt game with delay: A representation of a FlipIt game where both players are playing periodically. Every move or flip is indicated by a blue or orange circle. The defender is represented in blue and plays with a period of δ_D. The flip of the attacker is represented by a white circle, but because there is a delay d, the attacker only controls the resource after time d represented by an orange circle. The attacker plays with a period of δ_A. The blue and orange rectangles represent the amount of time the respective player is in control of the resource. 17

3.2 Case 1: Difference between a basic FlipIt game and a FlipIt game with a delay. (1) is the FlipIt game without a delay and (2) is with a delay. The delay is denoted with an arrow. The attacker is only in control when the circle becomes orange. 19

3.3 Case 2 where d + deltaA < deltaD 21

4.1 This figure shows the three subcategories of each case. 'A' stands for Case 2.A: $\delta_D \geq d + \delta_A \geq \delta_A$ and 'B' stands for Case 2.B: $d + \delta_A \geq \delta_D \geq \delta_A$ 24

Lijst van tabellen

1 hiërarchie van de klassen van de strategieën in Flipit viii

2.1 Hierarchy of Classes of strategies in FlipIt 12

Hoofdstuk 1

Introduction

1.1 Introduction

Situation

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? Many businesses store confidential information on clients, which can be lost and possible be abused by competitors through data leakage. Also, disruption caused by distributed DoS attacks, may results in businesses failing to meet their service-level agreements. Ultimately, system and network security helps protecting a business's reputation, which is one of its most important assets.

A particular kind of threats are Advanced Persistent Threats (APT). An APT is a targeted cyber attack that is designed to penetrate a network or a system in a stealthy way and that can stay undetected for a long period. This makes it so hard to protect a network or a system against an APT. Bruce Schneier describes an APT as something different and stronger than a conventional threat: "*A conventional hacker or criminal is not interested in any particular target. He wants a thousand credit card numbers for fraud, or to break into an account and turn it into a zombie, or whatever. Security against this sort of attacker is relative; as long as you're more secure than almost everyone else, the attackers will go after other people, not you. An APT is different; it's an attacker who - for whatever reason - wants to attack you. Against this sort of attacker, the absolute level of your security is what's important. It does not matter how secure you are compared to your peers; all that matters is whether you're secure enough to keep him out*" - Bruce Schneier [1].

misschien meer zeggen over APTs en threats

Complication

Since it is so difficult to protect a system or a network against APT's, researchers have been looking for effective ways to predict in advance which defence strategy might be the better one. Game theory is gaining increasing 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, van Dijk et al, made a game theoretic model of targeted attacks. They study the specific scenario where a system or network is repeatedly taken over completely by an without being immediately detected by the defender of the system or network. In game theory, such a game is known as "FlipIt" [12]. 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 immediate 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 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.

Research questions

The game theoretical approach of the FlipIt does not take such delay into account. This an lead us to the following research questions:

- How can we incorporate the notion of delay in the game-theoretical analysis of the Flip-It game for a periodic strategy ?
- Is there an optimal defense strategy against an attacker ?

Contributions

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 ..

Overview of the thesis

–opbouw van de thesis uitleggen–

The organisation of this paper is the following. In chapter 2 a brief introduction to Gametheory is introduced to get familiar with the game theoretic concepts that

will be further used in the paper. In the same chapter the FlipIt framework is summarized and the most important conclusions together with the the related work done on FlipIt and the difference with this paper. In chapter 3 , we first introduce the adaptations made on FlipIt to model a FlipIt game with virus propagation. After that formulas are derived to model a FlipIt game with a virus propagation for a specific case where players play a periodic strategy with a random phase. This chapter ends with simulations where conclusions can be derived. Next in Chapter **??** we given an overview of the various ways in which a virus can propagate. We present a method to calculate the speed of the propagation of a virus in a network and how this network can be established to reduce the spreading of a virus. Finally, in Chapter 5 , we discuss the main results and complications and provide directions for further research.

Hoofdstuk 2

Intoduction to GameTheory

This chapter provides the reader with an introduction to the general context of the work presented in this paper. Section 2.1 introduces the reader into the basic concepts of cyber security and the kind of cyber security threaths that are in the scope for this work. Section 2.2 then introduces the reader into the main principles of game theory. Subsequently, section 2.3 introduces the reader to the FlipIt game, the specific game that will be used to model cyber security attacks of periodic nature and including a delay. Finally, section 2.4 gives an overview of the related work, and how the research presented in this thesis is positioned compared to existing results.

2.1 What is cyber security?

Before the digitalization of documents, information was kept on paper and the security of this information was ensured by administrative and physical means. For example, you needed a key to access documents stored in a room full of cabinets where the files were kept. In today's digital era more and more information is kept in a digital format, stored on a computer. As digitalization progressed, the need for ensuring the security of digital information arose and automated tools where developed for protecting files stored on a computer. The generic name to protect data stored on a computer controlled device such as computers and smartphones, as well as public and private computer networks, including the entire Internet is called computer security.

Security is a general term that encompasses several dimensions. More specifically, computer security has tree key objectives that are fundamental to computer security:

Confidentiality: This assures that the confidential of private data is not disclosed or made available to users that do not have the authorization.

Integrity: This assures that data can not be altered by an unauthorized individual.

Availability: This assures that data is always accessible and that the service is not denied to authorized individuals.

the purpose of security is to give certainty that data will not be removed without authorization (Confidentiality) that the data is always accessible (Availability), and that data can not be read or altered by someone who does not have the authorization (Integrity).

These are the 3 key attributes of security, also known as the CIA triad. The tree concepts are fundamental security objectives for the securing of data, information and computing services.

"Cyber security is the process of applying security tools to ensure confidentiality, integrity, and availability of data. Cybersecurity attempts to ensure the protection of assets, which includes data, desktops, servers, buildings, and most importantly, humans. The goal of cyber security is to protect data both in transit and at rest. Countermeasures can be put in place in order to increase the security of data. Some of these measures include, but are not limited to, access control, awareness training, audit and accountability, risk assessment, penetration testing, vulnerability management, and security assessment and authorization."

tekst overgenomen van wikipedia

In the context of cyber security, the terms ' threat and attack' are often used interchangeably, referring to more or less the same thing. They however have a slightly different meaning. A threat refers to anything that can breach the security and that can cause a possible harm. It is a possible danger that can exploit a vulnerability. An attack is an assault on computer security that comes from a threat. It is an intelligent act that tries deliberately to breach security through vulnerabilities.

In order to keep a system secure, it is important to mitigate the possible threats. The possible threats can take many forms, the most commen being spam, malware, spoofing, phishing and DDoS attacks. A security report of 2014 reveals that 61% of the attacks on companies are caused by malware. This is a piece of malicious program that is designed to penetrate unprotected systems or computers, and getting there to sensitive information. Malware can be divided into different subclasses that are not mutually exclusive:

Virus: This is a malicious piece of code that replicates and tries to spread to infect other systems or files. The "I love you"virus is an example of a virus that quickly spreads. This virus propagates via mail systems. If someone opens an email with "I love you"with the virus in the annex this virus spreads itself by sending a mail to everyone in your contact list. So the virus can multiply rapidly and eventually a business network might shut down by the heavy traffic. In this example, there is a need for human interaction to spread the virus. If no one opens the mail the virus can not infect other systems. Unfortunately, there are also 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. Via a computer network, copies of the worm can be forwarded without an intermediary. The worm will use vulnerabilities of the system to infect other 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 to harm 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.

Rootkit: A rootkit is designed to be stealthy and hide a set of programs installed on a system from methods of detection. The programs have administrator or root privileges to that system, which makes it possible to access the functions and services of the operating system, change files, take control over the monitor processes and send and receive network traffic. A rootkit can make changes to the system to keep itself concealed from detection.

Trojan: This is a malicious program that disguises itself as something normal, so that users won't be suspicious of installing it.

Backdoors: Also know as trapdoor, is a whole in the system or program that allows access

A company can take different measures to defend itself against malware. The threats caused by malware can be divided into three main categories: known threats (70%), unknown threats (29%) and advanced threats (1%) as proposed by Kasperksy [].

toevoegen referentie naar kaspersky APT report

The known threats are the easiest to defend oneself against. Standard malware protection tools like firewalls and virus scanners can keep these kind of malware out of the system. Installing protection against unkown is also relatively easy. Then the remaining 1% are the advanced threats, also known as APT. APT's are ... In this paper we focus on targeted attacks. Targeted attacks are malware designed to attack exclusively an organisation.

An APT is a persistent targeted attack that tries to penetrate a network to harm it while staying unseen for a long period of time. The motive of an APT is mostly cyber espionage, stealing sensitive data, sabotage or some other kind of ideological attacks. Advanced Persistent Threat are called 'Advanced' for the fact that these attacks are well funded and that (usually) the attacker itself needs a great expertise to successfully penetrate a network. Not all APTs are technical advanced though. The attacker can also try to exploit existing vulnerabilities simply based in the hope that his target has not yet secured himself against these vulnerabilities. 'Persistent' refers to the fact that the attacker keeps on trying to break in to his victim. He will not give up. The attack can be over various years and different steps. The threats stands for the fact that an APT is attempting to break the protection of valuable data the leakage of which outside the secure environment may severely damage the organisation owning the data.

Some examples of the biggest most rare APTs are listed to get an understanding of what APTs are capable of and how long they can stay unseen. []

site kaspersky apt

Equation

Equation is a complex cyberattack platform where the first known sample is from 2002, but it was only discovered 12 years later in 2014. This APT propagates through usb drives, cd or physical media. It will search for exploits and will self-replicate itself to spread the infection. The purpose of this virus is to steal data and cyberespionage.

Regin

Flame

Way of propagation through USB drives, LAN spreading. purpose cyber espionage.

Black energy

purpose cyber espionage and DDoS, data wiping. prop usb lan

APT report

According to [] the damage of one successful target attack can exceed over 2.54 million dollar. a company needs a defense mechanism to defend itself against apt. Prevention more important than .. een van de manieren om dat te doen is via game theorie.

Security belangrijk. verschillende malware. uitleggen malware. verwijzen naar kaspersky security raport. APT grote threats. voorbeelden van APT's. waarom gametheory gebruiken.

2.2 Intro game theory

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 [8] and [3] is given in section 2.3 . For a more detailed and full introduction to game theory, the reader is referred to [8]. In section 2.4 an overview of the FlipIt game is given with the definitions and concepts that will be used throughout the paper. The last section 2.5 will cover the extensions and additions already made on FlipIt.

2.3 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. It has therefore important applications in many area's such as economics, 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 that tells how much an agent likes or dislikes the states of the world.
In a Decision Game Theoretic Approach an agent will try to act in such a way to maximise his expected or average utility function. It becomes more complicated when two or more agents want to maximise their utility and when actions of the agents can affect each other's 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.

2.3.1 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. To define this concept we first introduce the concept of best response. The best response for a player is the action of a player that maximizes it's pay-off for any given action of the other player. We define BR_i as the best response function for player *i*. The best response for player *1* is given by : $a_1 = BR_1(a_2)$. A For a Nash Equilibrium each player has a consist list of actions and each player's action maximizes his or her pay-off given the actions of the other players. Nobody has the incentive to change his or her action if an equilibrium profile is played. We have a Nash Equilibrium for the pair (a_1^*, a_2^*) where $a_1^* = BR_1(a_2^*)$ and $a_2^* = BR_2(a_1^*)$

optimal strategy uitleggen

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

List of terms

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.

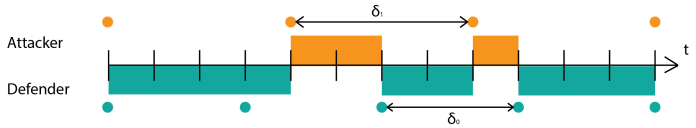
2.4 The FlipIt game

FlipIt is a game introduced by van Dijk et al. 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 its notations. Therefore, we first explain the framework of FlipIt and introduce the most important formulas that will be used throughout the paper.

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 remainder 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 continues indefinitely ($t \to \infty$). The time in the game is assumed as being continuous. To get control over the resource, the players i, with $i \in \{A, D\}$, can flip the resource at any given time. Each move implies a certain cost k_i and can vary for each player. Both players try to minimize their cost. Adding a cost prevents players to move too frequently.

The unique feature of FlipIt is that every move happens in a stealthy way, meaning that the player has no clue that the other player (his adversary) has flipped the resource. For instance, the defender does not find out if the resource has been compromised by the attacker until 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 the 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 player. If the player 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, so the cost is wasted.



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

We denote the state of the resource as a time-dependent variable $C = C_i(t)$. $C_D(t)$ is 1 if the game is under control by the defender and 0 if the game is under control by the attacker. Reversely, $C_A(t)$ is 1 if the game is under control by the

attacker and 0 if under control by the defender. So, $C_A(t) = 1 - C_D(t)$. The game starts with the defender being in control: $C_D(0) = 1$.

The players receive a benefit equal to the time units 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:

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

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 rate 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 given 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.

$$\beta_i(t) = \lim_{t\to\infty} inf\beta_i(t) \tag{2.6}$$

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 feedback for either player, we have a non-adaptive strategy. Because a player does not receive any feedback during the game he will play in the same manner against every opponent. The strategy is called non-adaptive because the playing strategy is not dependent on the opponents movements. An interesting subclass of the non-adaptive strategies is the one where the time intervals between

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

Tabel 2.1: Hierarchy of Classes of strategies in FlipIt

two consecutive moves are generated by a renewal process. An example of such 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. In case there is feedback, a player can adapt his strategy to the information received about the opponent's moves. Depending on the amount of information received, two subclasses of adaptive strategies can be identified. The Last Move (LM) strategies represent the class where whenever a player flips he will find out the exact time that the opponent played the last time. In the second class, called Full History (FH), whenever a player flips he will find out the whole history of the opponent's move. In this paper we restrict ourselves to periodic strategies. This choice is motivated by the fact that in a security game a player (defender or attacker) rarely has information about the moves (last move or full history) of his opponent.

Results of the FlipIt game

The study of the different strategies by means of FlipIt framework allows to derive a number of interesting results:

- periodic games dominate the other renewal strategies, meaning that it is always advantageous to play periodically against an opponent with a renewal strategy;
- periodic games are disadvantageous against players following a Last Move adaptive strategy;
- if the defender plays with a periodic rate that is fast enough he'll force the attacker to drop out;
- any amount of feedback about the opponent received during the game, benefits to a player.

2.5 Extensions on FlipIt

Various possible ways to extend FlipIt have already been proposed. Laszka et al. made a lot of additions and extensions to the original game of FlipIt. For instance

Laszka et al. extended the basic FlipIt game to multiple resources. The rationale is that for compromising a system in real life, more than just one resource needs to be taken over. An example is that gaining access to deeper layers of a system may require breaking several passwords. The model is called FlipThem [5]. Laszka et al. also 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 [6] 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 additions from Laszka et al. [7] is to consider a game with targeted and non-targeted attacks where the moves made by the attacker do not succeed immediately. This is similar to this paper but it has still some major differences. First the moves by the attacker are still covert but the moves made by the defender are known to the attacker. This means that the attacker knows when the defender plays and can change its strategy depending on the moves of the defender. Our motivation for a defender with stealthy moves is that there is not always an intelligent individual that is behind an APT. Some APTs don't know if the computer is already been recovered. There purpose is to spread. Not to check if they have already infected. . The second difference is that even though both the targeted and non-targeted attacks do not succeed immediately, the delay is determined differently. 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. In our paper the delay is given by one parameter, that can be the result of any virus propagation model. The third and last difference is that the paper of Laska has multiple attackers and they try to find the best strategy of the defender against both targeted and non-targeted attacks. The conclusion of this paper is that the optimal strategy for the defender is moving periodically.

beter verwoorden

FlipIt has also been applied to several cases in system security. Reseachers explored different applications of FlipIt for real-world problems, like password reset policies, VM refresh, cloud auditing and key rotation [4].
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 [10] 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.
A three-player game has also been investigated where the flipit framework of two players is extended by another player. This player represents an insider that trades

value information with the attacker [**?**].

Finally researchers also have investigated the behaviour of humans playing FlipIt. A. Nochenson and Grossklags [9] investigate how people really act when given temporal decisions. They found out that the results improves over time but that they are dependent on gender, age, and other individual difference variables. The result also shows that the participants perform generally better when they have more information about the strategy of the opponent which is a computerized player. Reitter et al. [11] extended the work of A. Nochenson and Grossklags to include various visual presentation modalities for the available feedback during the investigation.

Hoofdstuk 3

FlipIt game with virus propagation

3.1 Introduction

The game of FlipIt with virus propagation considers attackers where their moves are not instantaneous. This can be motivated by an example of a virus. A virus can be dropped on a network but it only compromises the whole network if every node in the network is infected. The basic FlipIt game does not take this into account. In this chapter the FlipIt game with virus propagation is explained and how it can be modelled. First the main differences with the basic FlipIt game are discussed in section 3.3. Next in section **??** the formal definition of the game with virus propagation is given. At last, in section 3.4 a periodic strategy game is considered and the formalization of the formulas with virus propagation are determined.

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.

3.2 FlipIt game with virus propagation

Motivation

3.3 Explaining difference between FlipIt with and without virus propagation

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 on the other hand 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 possible time. After dropping a virus on the first node, it takes a while for the virus to infect the entire network. 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 gain immediate full control over the resource when the network has been infected, even it is only one node that has been infected.

In reality however, after dropping a virus on the first node, it takes a while for the virus to infect the entire network. So, the assumption that the attacker has full control over the resource as soon as a node has been infected, is not realistic. The attacker has only control of the network once all or a sufficient number of nodes are infected. The time that it takes for the virus to infect every node (or a sufficient number of nodes) will be denoted as an infection-delay variable d (called 'delay' for short in the remainder of this paper). 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. Rather than denoting the time needed for infecting *all* the nodes, the variable d can also be used to denote the time needed to infect *a sufficient number* of nodes.

Assume that an attacker attacks at time t, he doesn't get immediate control over the resource, but he only gains control at time $t + d$, with d denoting the time needed to infect a sufficiently number (or all) nodes. 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 full control over the resource. This implies that the mathematical formulas for gain and benefit need to be adapted to the fact that the attacker loses part of its benefit because of this delay. In the remainder of this paper, we will adapt the formalization of the FlipIt game using the variable d.

3.4 Playing periodically with virus propagation

The formalization starts from the model of the non-adaptive continuous basic FlipIt game where players use a periodic strategy with a random phase. This choice is motivated by the assumption that in most organisations, the defence strategy is to periodically defend the network. This corresponds to a periodic defender strategy. A periodic attacker strategy is assumed as well, to be able to compare the results with the periodic strategy of the FlipIt game in [12]. Further research can investigate the effect of relaxing this assumption.

Similarly as in [12], we split the formalization in two cases. The first case is where the defender plays at least as fast as the attacker, the second case is where the attacker plays at least as fast as the defender. For each of these cases, first the benefit formula of the basic case without delay is presented, and then the delay is

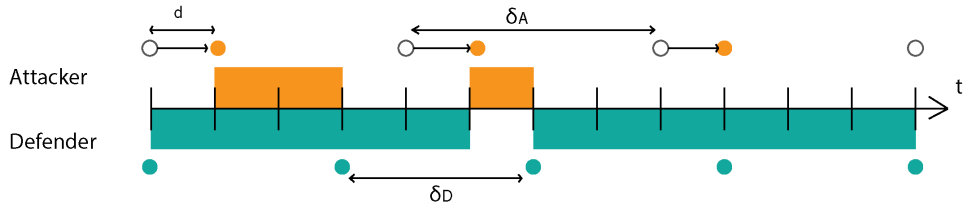
introduced.

Intuitively we could assume that d can never be bigger than δ_A because then the benefit for the defender would always be 1. This is not always true. It is only true if d is bigger than δ_D, because then the defender will always be in control. For this we only calculate the formulas for the cases where d is smaller than δ_D. We can already conclude that it is no use for the attacker to play when the delay is bigger than δ_D.

3.4.1 Formalization the benefit formula including the infection-delay

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 of a player is denoted by $\alpha_i = \frac{1}{\delta_i}$. List of symbols that will be used throughout the paper. Figure 3.1 represents a couple of the symbols for clarification.

FIGUUR 3.1: Formalization of a FlipIt game with delay: A representation of a FlipIt game where both players are playing periodically. Every move or flip is indicated by a blue or orange circle. The defender is represented in blue and plays with a period of δ_D. The flip of the attacker is represented by a white circle, but because there is a delay d, the attacker only controls the resource after time d represented by an orange circle. The attacker plays with a period of δ_A. The blue and orange rectangles represent the amount of time the respective player is in control of the resource.



i: Defines the player. Different as in the FlipIt paper where the defender is denoted by the subscript 0 and the attacker by the subscript 1.

δ_i: The length of the interval between two consecutive moves of player i.

α_i: The average flip rate of player i, given by $\alpha_i = 1/\delta_i$.

k_i: The cost of player i's moves.

d: The delay caused by the virus propagation.

$G_i(t)$: The total gain of player i denotes the amount of time player i is in control over the resource up to time t.

γ_i: The average gain rate of player i defined as $G_i(t)/t$

β_i: The average benefit rate up to time t defined as $\beta_i = \gamma_i - k_i\alpha_i$.

opt_i: The optimum function.

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

Let $r = \frac{\delta_D}{\delta_A}$. 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 by a virus. Therefore the benefit for the attacker, without considering the delay, can be expressed as follows:

$$\beta_A(\alpha_D, \alpha_A) = \frac{r}{2} - k_A\alpha_A = \frac{\delta_D}{2\delta_A} - k_A\alpha_A$$

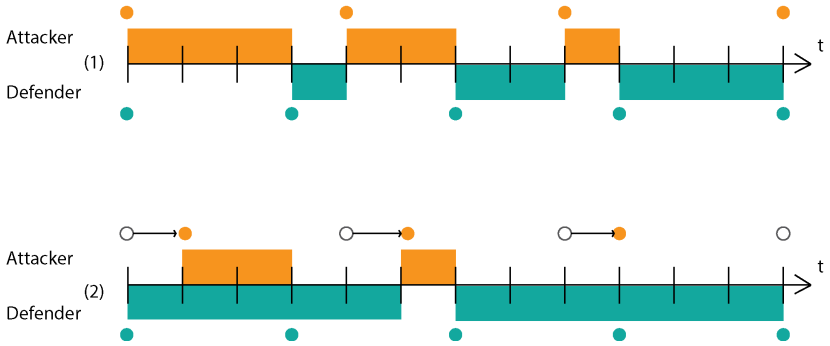
Correspondingly, the benefit for the defender can be expressed as:

$$\beta_D(\alpha_D, \alpha_A) = 1 - \frac{r}{2} - k_D\alpha_D = 1 - \frac{\delta_D}{2\delta_A} - k_D\alpha_D$$

However, because of the delay required for virus propagation, the maximal time of control is reduced to $\delta_D - d$, see figure 3.2. There is a probability of r that the attacker will move in the interval of the defender. However, the gain will not be half of the interval. Indeed, 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. The probability that the attacker plays soon enough is $\frac{\delta_D - d}{\delta_D}$ and this will give the attacker an average gain of $\frac{\delta_D - d}{2}$. If the attacker moves after the period of $\delta_D - d$, the gain of the attacker will be zero. The probability that this happens is $\frac{d}{\delta_D}$. The average gain rate of the attacker can then be expressed as follows if we look at one interval of the defender:

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

FIGUUR 3.2: Case 1: Difference between a basic FlipIt game and a FlipIt game with a delay. (1) is the FlipIt game without a delay and (2) is with a delay. The delay is denoted with an arrow. The attacker is only in control when the circle becomes orange.



To derive the benefit, the cost of moving is subtracted from the average gain.

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

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

The benefit of the defender is expressed as follows:

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

We can easily see that when d=0, we obtain the formula of the original FlipIt game.

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

First 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 $\frac{\delta_A}{\delta_D} = (1/r)$. Given that the defender moves within the interval of the attacker, he moves exactly once within this interval (since $\delta_A \leq \delta_D$) and his move is distributed uniformly at random.

A similar analysis as in case 1 for a FlipIt game without virus propagation yields the following benefits:

$$\beta_D(\alpha_D, \alpha_A) = \frac{1}{2r} - k_D \alpha_D = \frac{\delta_A}{2\delta_D} - k_D \alpha_D$$

$$\beta_A(\alpha_D, \alpha_A) = 1 - \frac{1}{2r} - k_A\alpha_A = 1 - \frac{\delta_A}{2\delta_D} - k_A\alpha_A$$

An intuitive solution for the case with a virus would be to subtract the benefit of the attacker received in each interval with the delay similarly as in case 1. This would give us the following formula if we derive it in the same way:

$$\beta_A = \frac{(\delta_A - d)^2}{2\delta_A\delta_D} - \frac{k_A}{\delta_A}$$

But this results in an overestimation. How closer δ_A/δ_D is equal to one, the better the approximation. If $\delta_A/\delta_D = 1$ the result is correct. This formula does not take into account that if the attacker was in control in the previous interval, the delay should not be subtracted, because the delay will not be in control of the defender. This means that we have to look at what happens in the previous interval.

From the defender we know that his moves are instantaneous. It is easier to calculate the benefit of the defender in this case. Because the defender moves slower than the attacker we know that if the defender moves during the interval of the attacker, he only moves once within this interval. The defender will move during the interval of the attacker with a probability of $\frac{\delta_A}{\delta_D}$. When this happens the defender will end with being in control at the end of the interval. In the next interval the attacker will have to regain control, meaning that during the delay, the defender stays in control, see figure 3.3 cases (1) and (2). The defender will keep the control over the resource in the next interval over a period of the delay, namely d.

Consider a timespan $\delta_A + d$, representing the attacker's interval followed by the delay period in his next interval. The defender will never move twice during this timespan because $\delta_A + d \leq \delta_D$. Because $d + \delta_A \leq \delta_D$ the next move of the defender in this second interval will never occur during the delay, meaning that the entire delay can be considered as an extra benefit resulting of a play in the previous interval. So, every time the defender plays, he will get an average gain of $\frac{\delta_A}{2}$ in the interval where he plays and in the next interval will always receive a extra gain of d, yielding a total average gain per interval of $\frac{(d + \frac{\delta_A}{2})}{\delta_A}$

For the case with a virus we consider two cases, Case a and Case b, depending on whether the delay is shorter or longer than the difference between the attacker's and the defender's period.

Case a: $d + \delta_A \leq \delta_D$

The total gain rate of the defender is then the probability that the defender will move during an interval of the attacker multiplied by the total average gain per interval:

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

$$\gamma_D(\alpha_D, \alpha_A) = \frac{\delta_A}{2\delta_D} + \frac{d}{\delta_D}$$

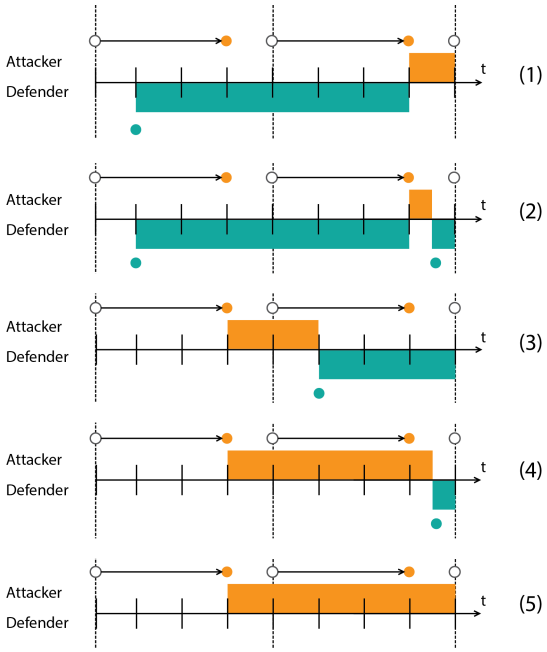
This yields in the following benefit formula:

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

The benefit for the attacker will be as follows:

$$\beta_A(\alpha_D, \alpha_A) = 1 - \frac{\delta_A}{2\delta_D} - \frac{d}{\delta_D} - k_A\alpha_A$$

FIGUUR 3.3: Case 2 where d + deltaA < deltaD



It is crucial that δ_D is at least as large as $d + \delta_A$. If not, this would mean that the defender can move during the delay in the interval following the interval where the defender already moved. This would mean that there can be an overlap between the average gain of $\frac{\delta_A}{2}$ and the delay. The above benefit formula would then include to

much gain for the defender: the potential overlap during the delay would be counted twice.

Case b: $d + \delta_A \geq \delta_D$

To obtain the formula in case of a too long delay, we therefore need to subtract this overlapping gain from the above formula. Since $\delta_D \geq \delta_A$, if the defender enters the interval immediately after the attacker has played, then the defender cannot have played in the previous interval. In that case, there is no overlap. So the problem of the overlap only appears if the defenders enters late enough and thus only the last part of the delay is subject to overlap. The larger the difference between the interval of the defender and the attacker, the smaller the risk of overlap. Concretely, only the last part of length $d - (\delta_D - \delta_A)$ is subject to overlap. Hence, the probability of overlap is $\frac{d - (\delta_D - \delta_A)}{\delta_D}$ and the gain will be half of this interval: $\frac{d - (\delta_D - \delta_A)}{2}$. The gain rate to be subtracted is therefore:

$$\frac{1}{\delta_A} \cdot \frac{d - (\delta_D - \delta_A)}{\delta_D} \cdot \frac{d - (\delta_D - \delta_A)}{\delta_D}$$

The total gain rate of the defender is obtained by subtracting this term from the gain rate of case a:

$$\gamma_D(\alpha_D, \alpha_A) = \frac{\delta_A}{\delta_D} \cdot \frac{(d + \frac{\delta_A}{2})}{\delta_A} - \frac{(d - (\delta_D - \delta_A))^2}{2\delta_D\delta_A}$$

$$\gamma_D(\alpha_D, \alpha_A) = \frac{\delta_A}{2\delta_D} + \frac{d}{\delta_D} - \frac{(d - (\delta_D - \delta_A))^2}{2\delta_D\delta_A}$$

This yields in the following benefit formula:

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

The benefit for the attacker will be as follows:

$$\beta_A(\alpha_D, \alpha_A) = 1 - \frac{\delta_A}{2\delta_D} - \frac{d}{\delta_D} - k_A\alpha_A + \frac{(d - (\delta_D - \delta_A))^2}{2\delta_D\delta_A}$$

Hoofdstuk 4

Nash Equilibria

4.1 Nash Equilibria

– rechtstreeks uit FlipIt paper –
As a second step, we are interested in finding Nash equilibria, points for which neither player will increase his benefit by changing his rate of play. More formally, a Nash equilibrium for the periodic game is a point (α_0^*, α_1^*) such that the defender's benefit $\beta_0(\alpha_0, \alpha_1^*)$is maximized at $\alpha_0 = \alpha_0^*$ and the attacker's benefit $\beta_1(\alpha_0^*, \alpha_1)$ is maximized at $\alpha_1 = \alpha_1^*$. To begin with, some useful notation. We denote by opt0(α_1) the set of values (rates of play α_0) that optimize the benefit of the defender for a fixed rate of play α_1 of the attacker. Similarly, we denote by opt1(α_0) the set of values (rates of play α_1) that optimize the benefit of the attacker for a fixed rate of play α_0 of the defender. The following theorem specifies Nash equilibria for the periodic game and is proven in Appendix A.

4.1.1 Determining the piecewise functions $opt_D(\delta_A)$

Nash equilibria are points with the property that neither player benefits by deviating in isolation form equilibrium. We can compute Nash Equilibria for the periodic game as an intersection points of curvest opt0 and opt1. To determine opt0(a0) we need to compute the derivative of $\beta_0(\alpha_0, \alpha_1)$ for a fixed α_1. We consider two cases:

Case 1: $\delta_D \leq \delta_A$

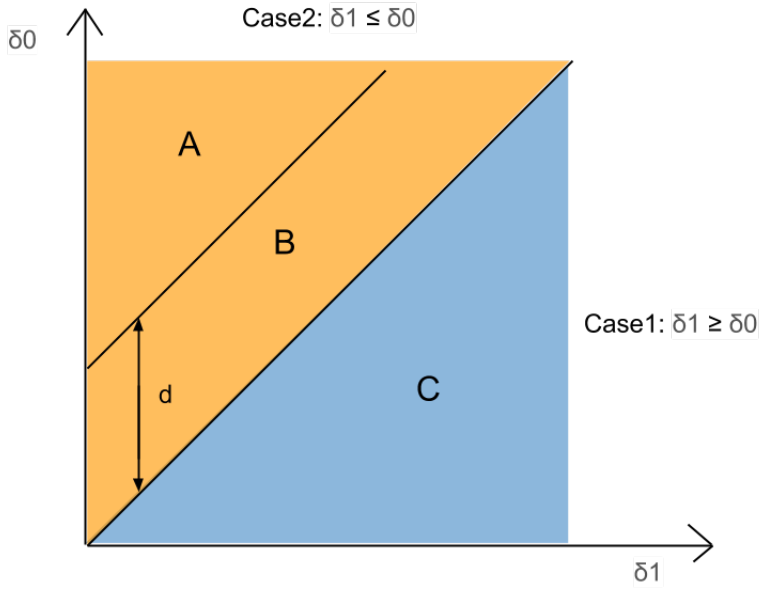
The benefit formula obtained previously for this case is as follows:

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

If we take the partial derivative for a fixed δ_1 we get the following result:

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

Figuur 4.1: This figure shows the three subcategories of each case. 'A' stands for Case 2.A: $\delta_D \geq d + \delta_A \geq \delta_A$ and 'B' stands for Case 2.B: $d + \delta_A \geq \delta_D \geq \delta_A$



The stationary points (maximum, minimum) can be found by setting the first derivative equal to zero and finding the roots of the resulting equation:

$$\frac{\partial \beta_D(\alpha_D, \alpha_A)}{\partial \alpha_D} = 0 \qquad => \qquad \delta_D = \sqrt{2\delta_A k_D + d^2}$$

This leads to the following deduction: The function increases on $[0, \sqrt{2\delta_A k_D + d^2}]$ and is decreasing on $[\sqrt{2\delta_A k_D + d^2}, \infty]$ So we got a maximum on $\delta_D = min\{\delta_A, \sqrt{2\delta_A k_D + d^2}\}$. The minimum of the two values is needed because δ_D cannot be bigger than δ_A.

Case 2.A: $\delta_D \geq d + \delta_A \geq \delta_A$

The benefit formula obtained previously for this case is as follows:

$$\frac{t\beta_D(\alpha_D, \alpha_A)}{\partial \alpha_D} = \frac{\delta_A}{2\delta_D} + \frac{d}{\delta_D} - \frac{k_D}{\delta_D}$$

The derivative of the above formula for a fixed δ_A results in the following:

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

The obtain the stationary points the first derivative is set equal to zero and the roots of the resulting equation are found:

$$\frac{\partial \beta_D(\alpha_D, \alpha_A)}{\partial \alpha_D} = 0 \qquad => \qquad \delta_A = 2(k_D - d) = dk_D - 2d$$

This leads to the following deduction:

If $k_D \leq d$

decreasing $\delta_A < 2(k_D - d)$

increasing $\delta_A > 2(k_D - d)$

If $k_D > d$

increasing $\delta_A < 2(k_D - d)$

decreasing $\delta_A > 2(k_D - d)$

Case 2.B: $d + \delta_A \geq \delta_D \geq \delta_A$

The benefit formula obtained previously for this case is as follows:

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

The derivative of the above formula for a fixed δ_A results in the following:

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

The stationary points (maximum, minimum) can be found by setting the first derivative equal to zero and finding the roots of the resulting equation:

$$\frac{\partial \beta_D(\alpha_D, \alpha_A)}{\partial \alpha_D} = 0 \qquad => \qquad \delta_D = \sqrt{2\delta_A k_D + d^2}$$

This leads to the following deduction: The function increases on $[0, \sqrt{2\delta_A k_D + d^2}]$ and is decreasing on $[\sqrt{2\delta_A k_D + d^2}, \infty]$ So we got a maximum on $\delta_D = minimum\{\delta_A, \sqrt{2\delta_A k_D + d^2}\}$

Best responses

The optimum functions will be piecewise functions. There will be different optimum functions depending on k_D and d. We distinguish for these two cases, three sub cases for different values of δ_A.

$k_D \leq d$

Because $k_D \leq d$, the term $2(k_D - d)$ will always be negative. We point out that δ_A and δ_D are positive rates.

- if $\delta_A < 2(k_D - d)$
  This means that δ_A has to be negative which is not possible. For case the defender will not play.
- $\delta_A = 2(k_D - d)$
  δ_A is negative or equal to 0 so the attacker will not play. For case 1 and case 2.b the defender will also not play.
- $\delta_A > 2(k_D - d)$
  Case 2.a it is increasing for every value $\delta_A \in [0, \infty]$. For case 1 together with case 2.b the optimal benefit is achieved at rate $\delta_D = \sqrt{d^2 + 2\delta_A k_D}$.

$k_D > d$

Because $k_D > d$, the term $2(k_D - d)$ will always be positive. We point out that δ_A and δ_D are positive rates.

- if $\delta_A < 2(k_D - d)$
  From case 2.a it follows that the benefit of the defender increases. From case 1 and case 2.b together the optimal benefit of the defender is achieved at rate $\delta_D = \sqrt{d^2 + 2\delta_A k_D}$.
- $\delta_A = 2(k_D - d)$
  From case 2.a it follows that $\beta_D(\delta_D, \delta_A) = 0$, for all $\delta_A \in [0, 2(k_D - d)]$. From case 1 and case 2.b together the optimal benefit for the defender is achieved for all rates $\delta_D \in [0, \sqrt{d^2 + 2\delta_A k_D}]$.
- $\delta_A > 2(k_D - d)$
  For case 2.a the benefit is decreasing. From case 1 and case 2.b the best strategy for the defender is not playing at all.

dat laatste nog eens nakijken

From this analyses we can compute $opt_D(\delta_A)$ for two different cases as:

$$opt_D(\delta_A) = \begin{cases} 0, & \delta_A < 2(k_D - d) \\ 0, & \delta_A = 2(k_D - d) \\ \sqrt{d^2 + 2\delta_A k_D}, & \delta_A > 2(k_D - d) \end{cases}$$

For case :

$$opt_D(\delta_A) = \begin{cases} \sqrt{d^2 + 2\delta_A k_D}, & \delta_A < 2(k_D - d) \\ [0, \sqrt{d^2 + 2\delta_A k_D}], & \delta_A = 2(k_D - d) \\ 0, & \delta_A > 2(k_D - d) \end{cases}$$

4.1.2 Determining the piecewise functions $opt_A(\delta_D)$

We still consider the case where $d < \delta_D$.
To determine the Nash equilibria we also need to determine $opt_A(\delta_D)$ by computing the derivative of $\beta_A(\delta_D, \delta_A)$ for a fixed δ_D. We consider 2 cases:

Case 1: $\delta_A \geq \delta_D$

The benefit formula obtained previously for this case is as follows:

$$\beta_A(\delta_D, \delta_A) = \frac{\delta_D}{2\delta_A} - \frac{k_A}{\delta_A} + \frac{d^2}{2\delta_D\delta_A^2} - \frac{d}{\delta_A}$$

The derivative for a fixed δ_D is as follows:

$$\frac{\partial\beta_A(\delta_D, \delta_A)}{\partial\delta_A} = -\frac{\delta_D}{2\delta_A^2} + \frac{k_A}{\delta_A^2} - \frac{d^2}{2\delta_D\delta_A^2} + \frac{d}{\delta_A^2}$$

The stationary points (maximum, minimum) can be found by setting the first derivative equal to zero and finding the roots of the resulting equation:

$$\frac{\partial\beta_A(\alpha_D, \alpha_A)}{\partial\alpha_D} = 0 \qquad => \qquad 2k_A = \frac{(\delta_D - d)^2}{\delta_D}$$

It follows that $\beta_A(\delta_D, \cdot)$ is increasing if $2k_A < (\delta_D - d)^2/\delta_D$ and decreasing if $2k_A > (\delta_D - d)^2/\delta_D$.

Case 2.A: $\delta_D \geq d + \delta_A \geq \delta_A$

The benefit formula obtained previously for this case is as follows:

$$\beta_A(\delta_D, \delta_A) = 1 - \frac{\delta_A}{2\delta_D} - \frac{k_A}{\delta_A} - \frac{d}{\delta_D}$$

The derivative for a fixed δ_D is as follows:

$$\frac{\partial\beta_A(\delta_D, \delta_A)}{\partial\delta_A} = \frac{-1}{2\delta_D} + \frac{k_A}{\delta_A^2}$$

The stationary points (maximum, minimum) can be found by setting the first derivative equal to zero and finding the roots of the resulting equation:

$$\frac{\partial\beta_A(\alpha_D, \alpha_A)}{\partial\alpha_D} = 0 \qquad => \qquad \delta_A = \sqrt{2\delta_D k_A}$$

it follows that $\beta_A(\delta_D, \cdot)$ is increasing on $[0, \sqrt{2k_A\delta_D}]$ and decreasing on $[\sqrt{2k_A\delta_D}, \infty]$ and thus has a maximum on $\delta_A = maximum\{\delta_D, \sqrt{2k_A\delta_D}\}$. The maximum between δ_D and $\sqrt{2k_A\delta_D}$ is needed because δ_A cannot exceed δ_D in this case.

Case 2.B: $d + \delta_A \geq \delta_D \geq \delta_A$

The benefit formula obtained previously for this case is as follows:

$$\beta_A(\delta_D, \delta_A) = 1 - \frac{\delta_A}{2\delta_D} - \frac{d}{\delta_A} - \frac{k_A}{\delta_A} + \frac{(d - (\delta_D - \delta_A)^2}{2\delta_D\delta_A}$$

The derivative for a fixed δ_D is as follows:

$$\frac{\partial\beta_A(\delta_D, \delta_A)}{\partial\delta_A} = -\frac{\delta_D}{2\delta_A^2} + \frac{k_A}{\delta_A^2} - \frac{d^2}{2\delta_D\delta_A^2} + \frac{d}{\delta_A^2}$$

The stationary points (maximum, minimum) can be found by setting the first derivative equal to zero and finding the roots of the resulting equation:

$$\frac{\partial\beta_A(\alpha_D, \alpha_A)}{\partial\alpha_D} = 0 \qquad => \qquad 2k_A = \frac{(\delta_D - d)^2}{\delta_D}$$

it follows that $\beta_A(\delta_D, \cdot)$ is increasing if $2k_A < (\delta_D - d)^2/\delta_D$ and decreasing if $2k_A > (\delta_D - d)^2/\delta_D$. This is the same result as in case 1.

Best responses

The optimum functions will be piecewise functions. We distinguish three cases for different values of δ_d and k_A.

For this term $\frac{(\delta_D - d)^2}{\delta_D}$, d has to be bigger than δ_D because the cost k_A cannot be negative. This was an assumption that was already made, because the benefit of the defender will always be 1 if d is bigger than δ_D.

- if $2k_A < \frac{(\delta_D - d)^2}{\delta_D}$
  Then for case 1 and case 2.b the benefit of the defender is increasing. From case 2.a follows that the optimal benefit for the attacker is achieved at the rate $\delta_A = \delta_D$

- if $2k_A = \frac{(\delta_D - d)^2}{\delta_D}$
  From case 1 and case 2.b it follows that $\beta_D(\delta_D, \delta_A) = 0$, for all $\delta_A \in [0, \frac{(\delta_D - d)^2}{2k_A})]$. From case 2.a the optimal benefit for the defender is achieved for all rates $\delta_A \in [0, \delta_D]$.

- if $2k_A > \frac{(\delta_D - d)^2}{\delta_D}$
  All decreasing.

Hoofdstuk 5

Conclusion

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

5.1 trala

Bibliografie

[1] Advanced persistant threats (apt).

[2] Standaard: Snowden bevestigt dat belgacom gehackt werd.

[3] Gametheory, 2004.

[4] K. Bowers, M. van Dijk, R. Griffin, A. Juels, A. Oprea, R. Rivest, and N. Triandopoulos. Defending against the unknown enemy: Applying flipit to system security. In J. Grossklags and J. Walrand, editors, *Decision and Game Theory for Security*, volume 7638 of *Lecture Notes in Computer Science*, pages 248–263. Springer Berlin Heidelberg, 2012.

[5] A. Laszka. Flipthem: Modeling targeted attacks with flipit for multiple resources. *5th International Conference, GameSec 2014, Los Angeles, CA, USA, November 6-7, 2014. Proceedings*, 8840:175–194, 2014.

[6] A. Laszka, B. Johnson, and J. Grossklags. Mitigating covert compromises. *iets*, 8289:319–332, 2013.

[7] A. Laszka, B. Johnson, and J. Grossklags. Mitigation of targeted and non-targeted covert attacks as a timing game. 8252:175–191, 2013.

[8] K. Leyton-Brown and Y. Shoham. *Essentials of Game Theory: A Concise, Multidisciplinary Introduction.* Synthesis lectures on artificial intelligence and machine learning. Morgan & Claypool Publishers, 2008.

[9] A. Nochenson, J. Grossklags, et al. A behavioral investigation of the flipit game. In *Proceedings of the 12th Workshop on the Economics of Information Security (WEIS)*, 2013.

[10] V. Pham and C. Cid. Are we compromised? modelling security assessment games. In J. Grossklags and J. Walrand, editors, *Decision and Game Theory for Security*, volume 7638 of *Lecture Notes in Computer Science*, pages 234–247. Springer Berlin Heidelberg, 2012.

[11] D. Reitter, J. Grossklags, and A. Nochenson. Risk-seeking in a continuous game of timing. In *Proceedings of the 13th International Conference on Cognitive Modeling (ICCM)*, pages 397–403, 2013.

[12] M. van Dijk, A. Juels, A. Oprea, and R. Rivest. Flipit: The game of "stealthy takeover". *Journal of Cryptology*, 26(4):655–713, 2013.

Fiche masterproef

Student: Sophie Marien

Titel: Flip the virus: Modelling targeted attacks using FlipIt with propagation delay

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. T. Holvoet

Assessoren: Prof. dr. B. Jacobs
Dr. ir. A. Dries

Begeleiders: Ir. Jonathan Merlevede,
Ir. Kristof Coninx