1 Extensions on FlipIt

There a various possible ways to extend FlipIt. For instance Laszka et al. extended the basic FlipIt game to multiple resources. The incentive is that for compromising a system in a real case it needs more than just taking over one resource. An example is gaining access to a system and breaking the password. The model is called FlipThem **?**. Two ways of flipping the resources are used: 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. The difference with FlipThem and this paper is that we introduce a Graph Model in the beginning.
Another extension on FlipIt is done by Pham**?** []. Beside the action Flip their is another action Test. The basic idea is to test with an extra action if the resource has been compromised or not. This action involves also an extra cost. This model is useful if somebody wants to know for example if his password has been compromised or wants to assess the periodic security of a system. In **? ?** Laszka et al. they also consider non targeted attacks by non-strategic players and .

citatie needed voor Are We Compromised?

verder aanvullen

In this section, we introduce the game FlipIt **?**. FlipIt is a game introduced by .. .. and Rivest. First we explain the framework of FlipIt and after that the formulas and assumptions that we will make for the game for during the whole paper.

2 The First Topic of this Chapter

FlipIt is a two-players game with a shared (single) resource that the players want to control as long as possible. The shared resource can be a password, a network or a secret key depending on the setting being modelled. In the rest of the paper we will call the players the Attacker and the Defender. To get the control over the resource, players can flip the resource at any given time. Each move will imply a certain cost. The unique feature of FlipIt is that the move will happen in a stealthy way, meaning that the other player has no clue that the other player has flipped the resource. For instance, the defender will not find out if the resource has already been compromised by the attacker, but he can only potentially know it after he flips the resource himself. The goal of the player is to maximize the time that he or she has control over the resource while minimizing total cost of the moves. Players won't move to frequently. A move can also result in a "wasted move", called a flop. It may happen that the resource was already under control by the defender. If the defender moves when he or she has already control over the resource, he or she would have wasted move since it does not result in a change of ownership.

Because the players move in a stealthy way, there are different types of feedback that a player can get while moving:

- Non-adaptive (NA): The player does not receive any feedback during the game while flipping.
- Last move (LM): When a player flips it will find out the exact time that the opponent played the last time.
- Full History (FH): When a player flips it will find out the whole history of the opponents move.

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

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

In our assumption the strategy of both players will be non-adaptive. None of the players has information of the strategy of the opponent.

3 Figures

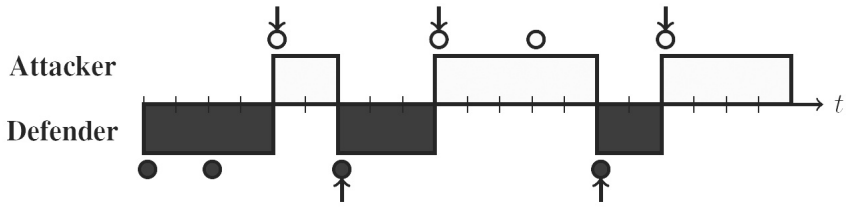

Figure 1: The FlipIt game where both players are playing periodically

verwijzen naar de figuur 1

3.1 Strategies

In this subsection we go through the strategies used in FlipIt and the most important results.

There are two different kinds of strategies, the *non-adaptive strategies* and the *renewal strategies*. If there is no need for feedback for both of the players, we say that we have a non-adaptive strategy. Because the player does not receive

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

Table 1: Classes of strategies in FlipIt

any feedback during the game it will play in the same manner against every opponent. They are not dependent on the opponents movements. This means that they can already generate the time sequence for all the moves in advance. But they can depend on some randomness because the non-adaptive strategies can be randomised. In this paper we will focus in the beginning on the non-adaptive strategies. Reasons behind this is that a player (defender or attacker) rarely knows what the strategies are of his opponent. [If the attacker wants to move stealthily, it might have limited attack options FLIPTHEM]. nog redenen zoeken
A renewal strategy is a non-adaptive strategy where the time intervals between two consecutive moves are generated by a renewal process.

Periodic

Non-Arithmetic Renewal

Exponential

4 Formal definition Game

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

Players There are two players in the game, one is the defender and the other one is the attacker. They are respectively identified by 0 and 1.

Time The game starts at $t = 0$ and continuous indefinitely as $t \to \infty$. The game is a continuous game.

Graph We represent the company network as a Graph $G =< V, E >$. G is an ordered pair where V denotes the set of resources or nodes in the network and E denotes the set of connections or links, which are a two-element subset of V. We use the notations resources and nodes interleaving in this paper.
We have N resources in the network. $N \in$. This means we can denote aanvullen
the resources by:

$$V \in V_0, V_1, V_2, ..., V_N$$

The set E of connections indicates if there is a link between two resources. We see the links as bidirectional so the total graph is undirected. If there is a link between resource V_n and V_{n+1} then there is also a link between V_{n+1} and V_n.

Game State There is also a time-dependent variable that represents the state of the game. $C = C(t)$ is either 0 if the game is under control by the defender and 1 if the Game is under control by the attacker.
We start at $t = 0$ with the defender who has control over the game. We do this because we assume that the defender will only put the network online without having a virus or worm in it. The Attacker can gain control over the game when it compromises a subset s of the resources. The subset s is a minimum of 1 resource and a maximum of all the resources N.
We can also define the state of each resource by C_N^A and C_N^D. If $C_N^A = 1$ then this means that the attacker has control over the resource, and 0 otherwise. For C_N^D it is visa versa, $C_N^D = 1 - C_N^A$.

deze variabele nodig ja of nee ? JA

Moves Both players can make a move in the game. Moves done in a finite numbers of time in any finite time interval. Both players can play at any time they want, they can also play at the same time. If this happens the one that has control over the resource will keep having control over the resource. This makes the game fully symmetric . The sequence of move times are denoted by the following infinite sequence:

beter uitleggen

$$t = t_1, t_2, t_3, ..$$

Two move times can be the same because we allow players to move at the same time. We can also denote the infinite sequence of times when player i moves. We write this as :

$$t = t_{i,1}, t_{i,2}, t_{i,3}, .. \text{ with } i \in \{0, 1\}$$

The sequences t_1 and t_0 are disjoint subsets of the sequent t. We can also denote who made the kth move by defining a sequence p that denotes the sequence of who played:

$$p = p_1, p_2, p_3, .. \text{ with } p_k \in \{0, 1\}$$

Number of moves $n_i(t$ denotes the number of moves made by player i up to and including time t. This means that

$$n(t) = n_1(t) + n_0(t)$$

is the sum of the number of moves made by the defender and the attacker up to and including time t.

Average move rate We denote $\alpha_i(t)$ as the average move rate by player i:

$$\alpha_i(t) = n_i(t)/t \text{ with } t > 0 \text{ and } i \in \{0, 1\}$$

Period We can also define the period in terms of the average move rate:

$$\delta_i = 1/\alpha_i$$

Who played last We know who played last by taking the modulo with the period. Z_i represents the time since the last flip of player i. We can also denote the time since the last flip of player i on resource r by Z_i^N. For a non adaptive game, period deterministic: At time $t = n$ is $Z_i = nmodi$. .

er kan nog steeds tegelijk geflipt zijn maar dan hebben ze wel geflipt

Cost The cost is an important property of the game. In FlipIt for every player the cost of a move is denoted by k_i. These costs can be very different for every player. In this game we denote the players flipping cost for resource V_N by $c_i^{V_N}$.
For the defender the cost will be either the cost of flipping every resource or the cost of flipping a subgroup of the resources.
For the attacker the cost will be the cost of dropping a virus on a node. The spreading of the virus will not imply an extra cost.

Utility In FlipIt the Gain definition is the utility function. The Gain denotes the total time a player i has gained control over a resource. The Gain G_i denotes players i total gain of a game, which is the total time the player has gained control over a subset of resources thus controlling the game. This is denoted by the following:

nu gain van een resource, moet voor verschillende resources zijn

$$G_i(t) = \int_0^t C_i(x)dx$$

If we sum up the total Gain of the attacker and the defender we end up with the time:

$$G_1(t) + G_0(t) = t$$

Average gain rate The average gain rate for player i is defined as

$$\gamma_i(t) = G_i(t)/t$$

4.1 Our Game parameters

Graph Matrix We represent the graph of the network through a matrix $A = |V| \times |V|$. The (i,j)-entry of the matrix A will have a 1 if there is a connection between node V_i and node V_j. If we are working with an undirected graph the matrix will be symmetric.

Attack Vector We denote $X = 1 \times |V|$ as the attack vector. It will be a vector with only zeros. The attacker will place a virus on a node V. This will be denoted by the Vth entry in the vector that is changed by a 1.

Reset vector The reset vector will make sure that the right entries in the matrix become zero. If the defender flips every node every time it

flips then the attack vector will be 0.

Cummulative Matrix This matrix will keep record of the propagation of the virus through the network.

State Matrix The State matrix $T(t) = 1 \times |V|$ will keep at every time t the state of the game and denote which node at time t is infected with the virus. At time $t = 0$ the State Matrix will be the null matrix.

De eerste infectie is de attack vector * Graph matrix .

4.2 Different kind of games

De virus has different kind of ways of making his way through the network. The virus can be dropped on a node and than spread itself out to all the neighbours. When a neighbour node is infected it will infect all its neighbours too, so the initial node is back infected. Then their are two options, either the initial node stays infected and does not infect all it neighbours again, or it does.
Another propagation method is that the virus works as a token. It will propagate to only one neighbour and continue to spread.

- A virus can use the mail system to spread itself. This will use then every contact in the contact list so it will spread itself to every neighbour
- If the virus does not want to get caught it can use the method of a path, infecting only one neighbour.
-

5 Conclusion

The final section of the chapter gives an overview of the important results of this chapter. This implies that the introductory chapter and the concluding chapter don't need a conclusion.