MŰEGYETEM 1782

Budapest University of Technology and Economics
Faculty of Electrical Engineering and Informatics
Department of Networked Systems and Services

Cyber-warfare with Game Theory

Semester Project 1.

Author
Zalán Nagy

Advisor
Dr. Gergely Biczók

May 25, 2025

1. Introduction and Motivation

Introduction

The aim of this thesis is to develop a two-phase game-theoretic model in which players simultaneously decide how to allocate their available resources. The model investigates under what conditions it is worthwhile to research one's own zero-day vulnerability as a function of the expected payoff. The optimization of the resource allocation strategies behind this decision constitutes the subject of this thesis.

The strategic importance of zero-day vulnerabilities has become an increasingly significant issue in cyber warfare and cybersecurity [1, 8, 9]. The game-theoretic approach offers a means of analyzing these complex decision-making situations, especially in contexts where state and nonstate actors employ hidden and advantage-seeking strategies [2, 7].

This research can contribute to supporting cyber-strategic decision-making and the development of defense policy guidelines. Analysis of game-theoretic equilibria can shed light on how certain parameters, such as the value of a zero-day vulnerability or the gain of a successful attack, influence players' decision preferences [10, 5].

Motivation

Zero-day vulnerabilities play an increasingly significant role in cybersecurity competitions, as these resources provide substantial advantages to attackers. However, discovering and exploiting zero-day vulnerabilities requires considerable resources, and thus strategic decisions regarding them deserve special attention.

Cyber arms races and attack/defense decision situations among various actors, be they state or private organizations, can be effectively modeled using game theory tools [7, 11]. Theoretical models, such as extensions of the Colonel Blotto game, are also suitable for analyzing resource allocation decisions [4, 3]. Analysis of player decisions, resource allocation strategies and the resulting equilibrium states can help to understand and predict the strategic processes that occur in cyberspace [6, 5].

2. The Game

2.1 Game model

There are two players: A and B. They are in a symmetric situation, meaning they have the same amount of resources available. These resources must be allocated between different strategic purposes. Both players are rational decision-makers, that is, they aim to maximize their own payoff. There is only one type of zero-day vulnerability in the model.

At the beginning of the game, each player has 1 unit of resource, which they can allocate in any proportion as follows:

$$r^X = r_z^X + r_a^X = 1$$

where:

- r_z^X is a discrete variable from the set $\{0;\ 0.5;\ 1\}$ – the amount of resource player X allocates to the discovery of zero-day vulnerabilities;
- r_a^X is a discrete variable from the set $\{0;\ 0.5;\ 1\}$ – the amount of resource player X allocates to "attack precision."

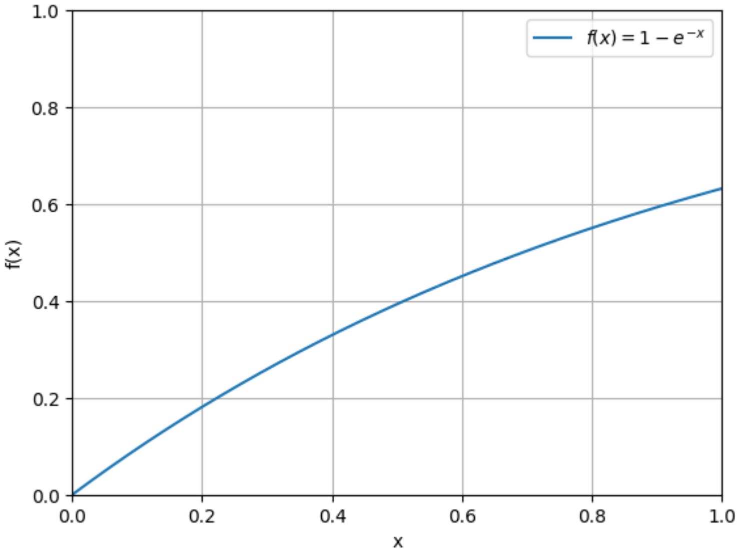
Note that due to the constraint $r_z^X + r_a^X = 1$, it is sufficient for the player to choose only one of the two values, which we denote here as r_z^X. In this case, the other value is determined as $r_a^X = 1 - r_z^X$.

If a player discovers a zero-day vulnerability, they will unconditionally launch an attack against their opponent.

Remark: originally, r_a^X represented the player's offensive power, but under the updated interpretation (as attack precision), a player can still launch an attack even when $r_a^X = 0$. It will become clear from the model that the values of r_a^A and r_a^B only matter if both players discover a zero-day vulnerability.

The probability of discovering a zero-day vulnerability is proportional to r_z^X. This discovery probability is given by the following function:

$$f(x) = 1 - e^{-x}$$



This particular function was chosen because, as players spend more on zero-day discovery, the marginal increase in discovery probability decreases – the relationship is clearly nonlinear. The function is increasing monotonically and asymptotically approaches 1. Intuitively, the probability of not discovering a zero-day is $1 - f(x)$. Hereafter, we refer to this as the function f, which takes the following values for the discrete inputs of r_z^X: $f(0) = 0$, $f(0.5) \approx 0.39$, $f(1) \approx 0.63$.

Let R be the reward gained for winning. To preserve symmetry, the winner gains $+R$, while the loser incurs a cost of $-R$.

If a player fails to discover a zero-day vulnerability, they only lose the resources invested in discovery, i.e., r_z^X. However, if a player launches an attack, they use all their resources, hence incur a cost of $r_z^X + r_a^X = 1$, regardless of the outcome.

If both players discover a zero-day vulnerability, the one who invested more in "attack precision" (i.e., has a higher $r_a^X = 1 - r_z^X$) wins the encounter, while the other player loses.

2.2 Graphical Illustration of the Game

The following graph illustrates the possible outcomes of the game.

See the figure: Figure A.1.

2.3 Payoff Functions

Let us define the payoff function for player A.

- If neither A nor B discovers a zero-day vulnerability, which happens with probability:

$$(1 - f(r_z^A)) \cdot (1 - f(r_z^B)),$$

  then no player can launch an attack, and A's cost is only the resources spent on zero-day discovery. Hence, A's payoff is: $-r_z^A$.

- If A fails but B discovers a zero-day, with probability:

  $$(1 - f(r_z^A)) \cdot f(r_z^B),$$

  then B attacks A. A's cost is $-r_z^A - R$.

- If A discovers a zero-day but B does not, with probability:

  $$f(r_z^A) \cdot (1 - f(r_z^B)),$$

  then A attacks B. The total cost to A is $r_z^A + r_a^A = 1$, and the gain is R, so the payoff is $R - 1$.

- If both players discover zero-day vulnerabilities, with probability:

  $$f(r_z^A) \cdot f(r_z^B),$$

  then the winner is determined by the attack precision. Player A's payoff is:

  $$\frac{r_a^A}{r_a^A + r_a^B} \cdot (R - 1) + \frac{r_a^B}{r_a^A + r_a^B} \cdot (-R - 1).$$

Taking these cases into account, the total payoff function for player A is:

$$\begin{aligned} U^A = &(1 - f(r_z^A)) \cdot (1 - f(r_z^B)) \cdot (-r_z^A) \\ &+ (1 - f(r_z^A)) \cdot f(r_z^B) \cdot (-r_z^A - R) \\ &+ f(r_z^A) \cdot (1 - f(r_z^B)) \cdot (R - 1) \\ &+ f(r_z^A) \cdot f(r_z^B) \cdot \left(\frac{r_a^A}{r_a^A + r_a^B} \cdot (R - 1) + \frac{r_a^B}{r_a^A + r_a^B} \cdot (-R - 1) \right). \end{aligned}$$

By symmetry, the payoff function for player B follows the same logic:

$$\begin{aligned} U^B = &(1 - f(r_z^A)) \cdot (1 - f(r_z^B)) \cdot (-r_z^B) \\ &+ (1 - f(r_z^A)) \cdot f(r_z^B) \cdot (R - 1) \\ &+ f(r_z^A) \cdot (1 - f(r_z^B)) \cdot (-r_z^B - R) \\ &+ f(r_z^A) \cdot f(r_z^B) \cdot \left(\frac{r_a^B}{r_a^A + r_a^B} \cdot (-R - 1) + \frac{r_a^A}{r_a^A + r_a^B} \cdot (R - 1) \right). \end{aligned}$$

2.4 Payoff Matrix

The players only need to decide on the value of r_z, since by definition $r_a^X = 1 - r_z^X$. From now on, we will focus solely on the choice of r_z.

We introduce a new notation to simplify the construction of the table. Let P^{ab} be the probability that players A and B have zero-day vulnerabilities, where $a = \{0, 1\}$ and $b = \{0, 1\}$. Here, $a = 1$ means that player A possesses a zero-day, and $a = 0$ means they do not. The interpretation for b and player B is analogous.

The probabilities are:

$$\begin{aligned}
P^{00} &= (1 - f(r_z^A)) \cdot (1 - f(r_z^B)) \\
P^{01} &= (1 - f(r_z^A)) \cdot f(r_z^B) \\
P^{10} &= f(r_z^A) \cdot (1 - f(r_z^B)) \\
P^{11} &= f(r_z^A) \cdot f(r_z^B)
\end{aligned}$$

The payoff matrix (with r_z^A on the left and r_z^B on the top) contains the possible decisions of the players and their corresponding payoffs. Each cell shows the first value as player A's payoff and the second value as player B's payoff. The detailed payoff matrix can be found in Table A.1 in Appendix A.

2.5 Searching for Nash Equilibrium as a Function of the Reward (R)

Note: In the calculations, values were mostly rounded to two decimal places. This introduces minor inaccuracies, but does not affect the essence of the solution.

We seek the best responses of player A to fixed decisions of player B.

When $r_z^B = 0$, the payoffs for A's possible decisions are:

- For $r_z^A = 0$:

$$u_A = 0$$

- For $r_z^A = 0.5$:

$$\begin{aligned}
u_A &= P^{00} \cdot (-0.5) + P^{10} \cdot (R - 1) \\
&= (1 - f(0.5))(1 - f(0)) \cdot (-0.5) + f(0.5)(1 - f(0)) \cdot (R - 1) \\
&= 0.61 \cdot (-0.5) + 0.39 \cdot (R - 1) \\
&= 0.39R - 0.695
\end{aligned}$$

- For $r_z^A = 1$:

$$\begin{aligned}
u_A &= P^{00} \cdot (-1) + P^{10} \cdot (R - 1) \\
&= (1 - f(1))(1 - f(0)) \cdot (-1) + f(1)(1 - f(0)) \cdot (R - 1) \\
&= 0.37 \cdot (-1) + 0.63 \cdot (R - 1) \\
&= 0.63R - 1
\end{aligned}$$

Since the payoffs depend on R, we seek the maximum among them. From the analysis:

- If $R < 1.59$, then the decision $r_z^A = 0$ yields the highest payoff.
- If $R > 1.59$, then $r_z^A = 0.5$ is the best choice.

Note: Further calculations are omitted.

When $r_z^B = 0.5$, the payoffs for A are:

- $r_z^A = 0$: $\quad u_A = -0.39R$
- $r_z^A = 0.5$: $\quad u_A = -0.695$
- $r_z^A = 1$: $\quad u_A = -1$

- If $R < 1.78$, then $r_z^A = 0$ is the best response.
- If $R > 1.78$, then $r_z^A = 0.5$ maximizes the payoff.

When $r_z^B = 1$, the payoffs for A are:

- $r_z^A = 0$: $\quad u_A = -0.63R$
- $r_z^A = 0.5$: $\quad u_A = -0.68$
- $r_z^A = 1$: $\quad u_A = -0.6$

- If $R < 0.95$, then $r_z^A = 0$ is the most favorable choice.
- If $R > 0.95$, then $r_z^A = 1$ yields the highest payoff.

Since the game is symmetric, the same cases apply to player B.

2.5.1 Equilibrium States Depending on R

From the previous calculations, we can distinguish seven different cases:

1. $R < 0.95$
2. $R = 0.95$
3. $0.95 < R < 1.59$
4. $R = 1.59$
5. $1.59 < R < 1.78$
6. $R = 1.78$
7. $1.78 < R$

For these cases, we examine separately the best responses and mutual best responses (Nash equilibria). A Nash equilibrium is a strategic situation where no player can unilaterally improve their outcome by changing their strategy given the other players' choices.

In the first case, when $R < 0.95$, player A always chooses $r_z^A = 0$ since it yields the highest payoff and changing the decision does not improve it. Similarly, B always selects $r_z^B = 0$ in this range. Thus, there is a single Nash equilibrium at $(0, 0)$.

In the second case, when $R = 0.95$, player A chooses $r_z^A = 0$ for $r_z^B = 0$ and $r_z^B = 0.5$, but for $r_z^B = 1$, both $r_z^A = 0$ and $r_z^A = 1$ yield the same payoff, so either can be chosen without incentive to deviate. The same reasoning applies to player B. This results in two Nash equilibria: $(0, 0)$ and $(1, 1)$.

The table below summarizes the Nash equilibria depending on R:

Value of R	**Nash Equilibrium States**
$R < 0.95$	$(0, 0)$
$R = 0.95$	$(0, 0); (1, 1)$
$0.95 < R < 1.59$	$(0, 0); (1, 1)$
$R = 1.59$	$(0, 0); (0.5, 0); (0, 0.5); (1, 1)$
$1.59 < R < 1.78$	$(0.5, 0); (0, 0.5); (1, 1)$
$R = 1.78$	$(0.5, 0); (0, 0.5); (0.5, 0.5); (1, 1)$
$1.78 < R$	$(0.5, 0.5); (1, 1)$

2.6 Conclusion

In this model, I examined how two symmetric players, each with the same amount of resources that they can allocate between zero-day vulnerability discovery and attack precision, choose their strategies under different reward values R. The outcome of the game depends on how the players divide their resources between discovery and attack and on the probability of successfully finding a zero-day vulnerability.

Nash equilibria are strategy combinations in which neither player has an incentive to unilaterally deviate from their chosen strategy, assuming that the other player maintains theirs. This means that such strategy pairs are stable: neither party can improve their own payoff simply by reallocating their resources. My calculations indicate that the equilibrium strategies are highly dependent on the magnitude of the reward.

For low values of R, it is not worthwhile for either player to invest significantly in discovery, as the potential gain from a successful attack does not compensate for the losses associated with the full expenditure of resources. In such cases, the Nash equilibrium corresponds to both players investing minimally (or not at all) in zero-day discovery, which represents a kind of passive strategy.

For higher values of R, the gain from a successful attack significantly exceeds the investment cost, making it advantageous for one or both players to allocate resources to discovery. In such scenarios, the Nash equilibrium may involve moderate or high levels of investment in discovery, with the likelihood of attacking the opponent increasing in parallel.

At certain intermediate values of R, players' strategies may become asymmetric despite the symmetric initial conditions. This phenomenon is known as spontaneous symmetry breaking, where players specialize into different roles: one focuses on discovery, while the other avoids it, and is thus less exposed to potential attacks. Such outcomes can also represent Nash equilibria if neither player would benefit from unilaterally changing their decision.

In summary, mapping the Nash equilibria helps us understand the circumstances under which aggressive behavior becomes more worthwhile and when it is more prudent to avoid fully utilizing available resources. This can be particularly important in modeling decision support systems for national security or cybersecurity, where similar types of strategic choices may arise.

3. Evaluation and Further Development Opportunities

The game model presented in this thesis provides a simplified framework for examining the dynamics of zero-day vulnerability discovery and attacks. The symmetric players and discrete resource allocation enable the analysis of strategic decisions as well as the exploration of Nash equilibria depending on the size of the payoff. The results highlight how players' resource-sharing decisions affect the chances of success and the outcomes of attacks.

3.1 Model Evaluation

The strength of the current model lies in its simplicity while capturing the essence of the trade-off between zero-day search and attack. The increase in success probabilities was modeled by a nonlinear function, which reflects well the diminishing returns observed in practice. The uniform allocation of one unit of resource and the discrete choice options allowed the creation of analytical expressions and payoff matrices.

However, the model can be further developed in several aspects to better approach the complexity of reality.

3.2 Further Development Directions

- **Refinement of resource allocation:** Currently, the choice options are discrete and limited ($\{0, 0.5, 1\}$). Introducing a more continuous resource-sharing scheme would enable more precise modeling, allowing players to allocate their resources between zero-day discovery and attack in any ratio.
- **Multiple types of zero-day vulnerabilities and attacks:** The model assumes a single zero-day vulnerability. In reality, multiple vulnerabilities of varying value or difficulty may exist, which require different amounts of resources to discover. Additionally, different types and efficiencies of attacks could be modeled.
- **Asymmetric players and resources:** The game currently assumes symmetric players. In real environments, actors have different capacities, resources, and motivations. Taking this into account, the model could be extended to asymmetric cases.
- **Multi-stage or dynamic game:** The current model is static, examining one-time decisions. A dynamic model that evaluates the zero-day discovery and attack process

over multiple time steps, or where players learn and adapt to opponents' strategies, would provide deeper insight.

- **Modeling risks and uncertainties:** Success probabilities were modeled deterministically. In real situations, uncertainty, randomness, and risks affect decisions in complex ways, which could be incorporated using stochastic models or Bayesian networks.
- **Communication and cooperation between players:** The possibility of cooperation or coalition formation in exploiting zero-days is an interesting further direction that could lead to new equilibrium states.

3.3 Summary

The game model developed in this thesis is well suited for examining the basic mechanisms of strategic decision-making in zero-day search and attack. Although simplified, it offers a clear and analyzable format that can serve as a good starting point for the development of more realistic models. By introducing further enhancements, the model's applicability can be significantly expanded, contributing to a deeper understanding of cybersecurity decision-making.

3.4 Personal Reflection

Throughout the semester, I continuously explored new game-theoretical concepts and possible modeling approaches. I reviewed numerous studies in the field, which significantly contributed to my professional development. Initially, I envisioned a much more complex model; however, over the weeks, I simplified it to ensure that I could complete a coherent and analyzable version within the semester. I believe that this topic holds considerable potential, and the model developed here lays the groundwork for further improvements. I am keen to continue working on similar subjects in future semesters as well.

Bibliography

[1] Louise Arimatsu. A treaty for governing cyber-weapons: Potential benefits and practical limitations. *Chatham House Reports*, 2012.

[2] John Arquilla and David Ronfeldt. Cyberwar is coming! *Comparative Strategy*, 1993.

[3] Enric Boix-Adserà, Benjamin L. Edelman, and Siddhartha Jayanti. The multiplayer colonel blotto game. *Games and Economic Behavior*, 2020.

[4] Pern Hui Chia and John Chuang. Colonel blotto in the phishing war. In *Workshop on the Economics of Information Security (WEIS)*, 2008.

[5] Benjamin Edwards, Alexander Furnas, Stephanie Forrest, and Robert Axelrod. Strategic aspects of cyberattack, attribution, and blame. *PNAS*, 2020.

[6] Marcelo M. Leal and Paul Musgrave. Hitting back or holding back in cyberspace: Experimental evidence regarding americans' responses to cyberattacks. *Journal of Conflict Resolution*, 2022.

[7] Tyler Moore, Allan Friedman, and Ariel D. Procaccia. Would a 'cyber warrior' protect us? exploring trade-offs between attack and defense of information systems. 2010. Position paper, Harvard University.

[8] Thomas Rid. Cyber war will not take place. *Journal of Strategic Studies*, 2012.

[9] Matthias Schulze. The state of cyber arms control. an international vulnerabilities equities process as the way to go forward? *SWP Research Paper*, 2017.

[10] Guizhou Wang, Jonathan W. Welburn, and Kjell Hausken. A two-period game theoretic model of zero-day attacks with stockpiling. *Journal of Cybersecurity*, 2023.

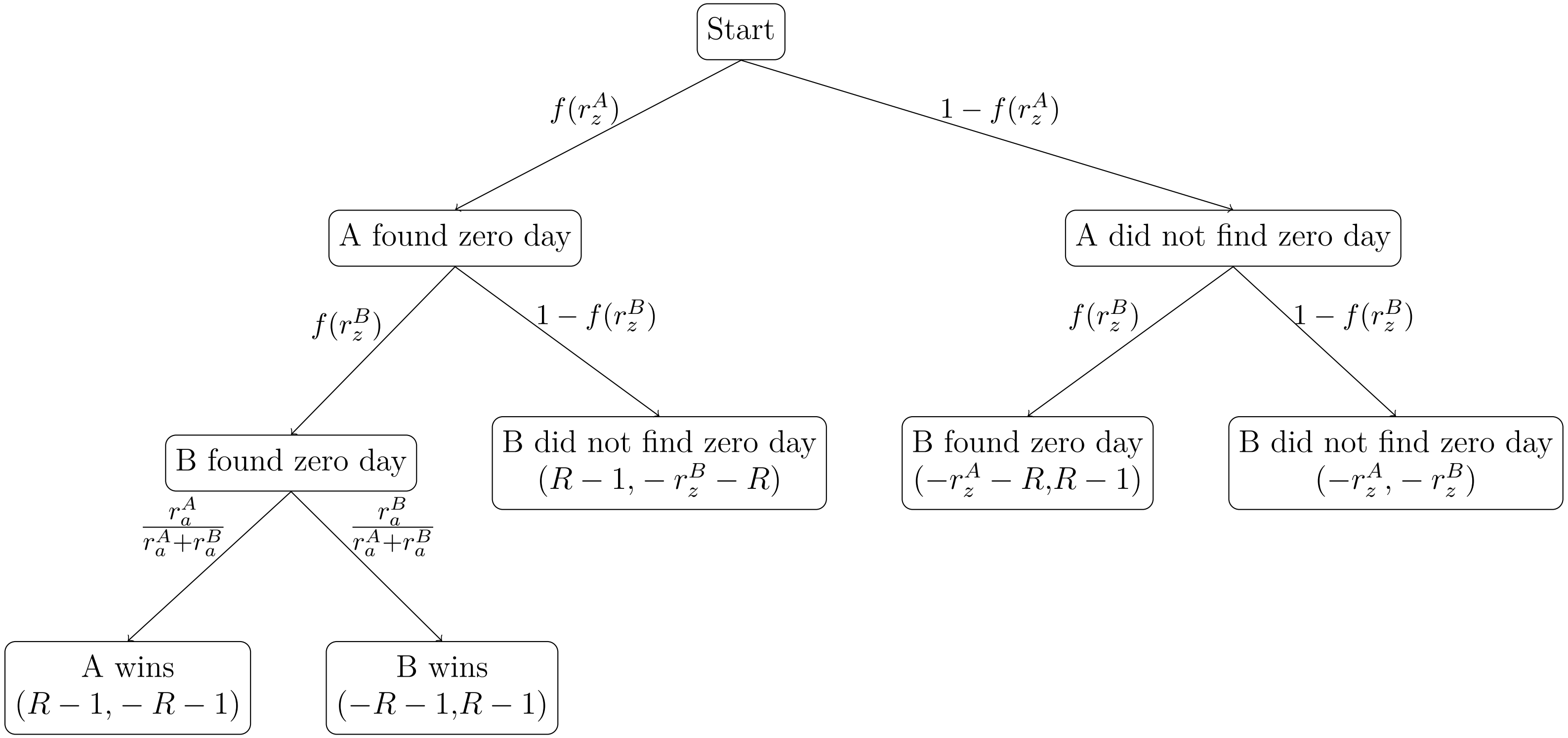
[11] Tongxin Yin, Armin Sarabi, and Mingyan Liu. Deterrence, backup, or insurance: Game-theoretic modeling of ransomware. *IEEE Transactions on Information Forensics and Security*, 2018.

Appendix A

Table A.1: The payoff matrix of the players

$r_z^A \backslash r_z^B$	**0**	**0.5**	**1**
0	0 0	$P^{01} \cdot (-R)$ $P^{00} \cdot (-0.5) + P^{01} \cdot (R-1)$	$P^{01} \cdot (-R)$ $P^{00} \cdot (-1) + P^{01} \cdot (R-1)$
0.5	$P^{00} \cdot (-0.5) + P^{10} \cdot (R-1)$ $P^{10} \cdot (-R)$	$P^{00} \cdot (-0.5) + P^{01} \cdot (-0.5-R) + P^{10} \cdot (R-1) + P^{11} \cdot (-1)$ $P^{00} \cdot (-0.5) + P^{01} \cdot (R-1) + P^{10} \cdot (-0.5-R) + P^{11} \cdot (-1)$	$P^{00} \cdot (-0.5) + P^{01} \cdot (-0.5-R) + P^{10} \cdot (R-1) + P^{11} \cdot (R-1)$ $P^{00} \cdot (-1) + P^{01} \cdot (R-1) + P^{10} \cdot (-1-R) + P^{11} \cdot (-R-1)$
1	$P^{00} \cdot (-1) + P^{10} \cdot (R-1)$ $P^{10} \cdot (-R)$	$P^{00} \cdot (-1) + P^{01} \cdot (-1-R) + P^{10} \cdot (R-1) + P^{11} \cdot (-R-1)$ $P^{00} \cdot (-0.5) + P^{01} \cdot (R-1) + P^{10} \cdot (-0.5-R) + P^{11} \cdot (R-1)$	$P^{00} \cdot (-1) + P^{01} \cdot (-1-R) + P^{10} \cdot (R-1)$ $P^{00} \cdot (-1) + P^{01} \cdot (R-1) + P^{10} \cdot (-1-R)$

Figure A.1: The decision tree of the game


Start
$f(r_z^A)$
$1 - f(r_z^A)$
A found zero day
A did not find zero day
$f(r_z^B)$
$1 - f(r_z^B)$
$f(r_z^B)$
$1 - f(r_z^B)$
B found zero day
B did not find zero day $(R-1, -r_z^B - R)$
B found zero day $(-r_z^A - R, R-1)$
B did not find zero day $(-r_z^A, -r_z^B)$
$\frac{r_a^A}{r_a^A + r_a^B}$
$\frac{r_a^B}{r_a^A + r_a^B}$
A wins $(R-1, -R-1)$
B wins $(-R-1, R-1)$