

UNIVERSITY OF WALES TRINITY SAINT DAVID

Bacterial Cyber Security - Energy Efficiency in Moving Target Defense Systems

by

Nathan Hughes

A project proposal submitted in partial fulfillment for the
degree of M.Sc. Applied Computing

in the

School of Applied Computing
Faculty of Architecture, Computing and Engineering

Supervisor: Mabrouka Abuhmida

May 2019

Contents

1	Introduction	1
1.1	Motivation - Systems with Static Defences	1
1.2	Moving Target Defence as a Solution	2
1.3	Energy Usage in Moving Target Defence	3
2	Background to the Proposed Research	4
2.1	Game-Theoretic Models	4
2.1.1	Markov Modelling of Moving Target Defense Games	4
2.1.2	A Game Theoretic Approach to Strategy Determination for Dynamic Platform Defences	5
2.1.3	Empirical Game-Theoretic Analysis for Moving Target Defense	6
2.2	Evolutionary Models	6
2.2.1	Evolutionary Based Moving Target Cyber Defense	6
3	Aims & Objectives	8
3.1	Mathematical Modelling	8
3.1.1	Choice of Moving Target Defences	8
3.1.2	Threat Model	8
3.1.3	Modelling Energy Usage	9
3.2	Experimental Simulation	9
3.2.1	Genetic Algorithms	9
3.2.2	Benchmarks	9
4	Research Methods	10
4.1	Philosophies & Strategies	10
4.2	Data Collection & Evaluation Methods	10
4.3	Reliability and Validity	11
4.4	Risks & Limitations	11
5	Resources & Planning	12
5.1	Resources Required	12
5.2	Gantt Chart	12
6	Conclusion	14
	Bibliography	15

Chapter 1

Introduction

1.1 Motivation - Systems with Static Defences

The current state of cyber security is dire, and this is explained no better than by exploit kits. Exploit kits are tools that automate the deployment of a collection of exploits, targeting the infection vectors of said exploits to install malware in the targeted computers [1]. In 2013, the exploit kit *Angler* was released [2]. Amongst other activities, users of Angler were able to:

1. exploit vulnerabilities of Adobe Flash and Internet Explorer [2, 3],
2. injecting redirecting POST methods into legitimate web pages pointing to malicious servers [2],
3. employ a technique called *domain shadowing* in which the Angler user compromises the account of a domain name registrant and create sub-domains that point to malicious servers [2–4].

Angler was brought to an end on the 6th of October 2015 by Cisco, but not before the kit had generated up to \$60 million of revenue for its users [3]. The implication of the existence of such software is clear - not only are they contributing to the cyber crime industry, but of particular note is the automatic nature of such kits. More recent research has shown that the sophistication of these kits has grown rapidly, to a point where the automation of the delivery of malware is now suited for mass proliferation through advertisements on web-pages, known as *malvertising* [5].

These exploits are able to be automated because the exploits are able to be re-used between systems. Often, these exploits remain hidden to the developers. It is unlikely

that any developments in computer security will ever address the existence of zero-day vulnerabilities directly. It is imperative, therefore, that these vulnerabilities are addressed indirectly. This project is concerned with such an approach.

1.2 Moving Target Defence as a Solution

A system implementing a Moving Target Defence technique is a system that makes its attack surface less static and homogeneous, giving the defender the same asymmetric advantage over time previously only granted to the attacker [6, 7]. A survey by Ward *et al.* taxonomically defined five moving target techniques that defenders could implement in their systems [8]. They are as follows:

Dynamic Data which changes the structure of data used by the application.

Dynamic Software which changes the code in the application.

Dynamic Runtime Environment which changes the environment offered by the operating system. Ward *et al.* sub-categorised this further, making a distinction between Address Space Randomization, which changes the layout of memory, and Instruction Set Randomization, which changes the interface offered by the operating system.

Dynamic Platforms which changes the properties of the platform on which the application runs, including but restricted to operating system version and architecture of the CPU.

Dynamic Networks which changes, for example, the protocols and addresses of the network.

As far back as 2009, researchers have recognised Moving Target Defence as a realistic strategy for defence, achievable with the innovations in technology currently available - key technologies include, but are not limited to, virtualisation, address space layout randomisation and Software as a Service offered by cloud providers [7].

It is important to note that the vulnerabilities of the technologies incorporated into a Moving Target Defence system are still present, however these vulnerabilities are less able to be exploited by attackers due to the evolving nature of the system.

1.3 Energy Usage in Moving Target Defence

Since the field of Moving Target Defence is relatively new, there are multiple questions left unaddressed. In particular, the resources used in the implementation of such defences has not been explored thoroughly. A paper by McDaniel *et al.* briefly explores this idea [9]. Resources used in a Moving Target Defence system can include computing costs, such as memory, available servers in a cloud infrastructure and power consumed. The proposed research will explore models for such resource consumption and propose Moving Target Defence techniques that will minimise the resources consumed.

Chapter 2

Background to the Proposed Research

The last chapter gave a motivation for Moving Target Defence, along with a definition and some brief examples. This chapter is a brief literature review of both the game theoretical and evolutionary modelling of Moving Target Defence systems. The purpose of this background research is to detail the attempts made at modelling Moving Target Defence systems, to highlight the similarities and differences, and to make clear the possible models that could be used for this project.

The first part of this chapter is a brief literature review of the game theoretical modelling of Moving Target Defence systems previously attempted. A simple description of the models constructed in these papers is given, along with an outline of the main results discussed by the authors. The second part of this chapter outlines the evolutionary models described in the literature.

2.1 Game-Theoretic Models

2.1.1 Markov Modelling of Moving Target Defense Games

This paper models a hacking scenario as a Markov Chain [10]. The game is defined by the Markov chain's transition matrix, from which the properties of the game are derived.

Definition 2.1. Let λ, μ be rates of play for the defender and attacker respectively, satisfying $0 \leq \lambda + \mu \leq 1$. Suppose the moving target defence technique has k degrees of freedom. Then a (M^D, λ, M^A, μ) -MTD game is based on the $(k + 1) \times (k + 1)$

transition matrices M^D, M^A , where $M_{i,j}^D$ is the probability of transitioning from state i to state j on the defender's turn, and similarly defined for the attacker.

The first example used in this paper illustrating this definition is that of *IP Address Randomization* moving target defence for a single target, in which the IP of the host on a network change dynamically. The degree of freedom here is the number of possible IP addresses the host can take. State 0 represents the initial state. When the attacker moves, they will guess an IP out of the possible IPs available. If successful, the Markov chain transitions to the winning state. If unsuccessful, the Markov chain transitions to the state above, representing the shortening of the pool of IPs left to guess. It is assumed the attacker does not second guess IP addresses until they have been exhausted. When the defence moves, with probability λ , the IP of the host will be changed. In terms of the Markov chain, this represents transition to state 0.

The corresponding (right) transition matrix is shown in 2.1.

$$\begin{pmatrix} 1 - \mu & \mu \frac{k-1}{k} & 0 & 0 & \dots & \mu \frac{1}{k} \\ \lambda & 1 - \mu - \lambda & \mu \frac{k-2}{k-1} & 0 & \dots & \mu \frac{1}{k-1} \\ \lambda & 0 & 1 - \mu - \lambda & \mu \frac{k-3}{k-2} & \dots & \mu \frac{1}{k-2} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & 0 & 0 & 0 & \dots & 1 - \lambda \end{pmatrix} \quad (2.1)$$

This was extended to cases of multi-target hiding, in which multiple hosts have their IP addresses dynamically changed.

The main theorem proved in this paper shows that, assuming a stationary distribution π for the Markov chain M exists, the probability that the attacker wins in the first T time steps is $T \cdot \pi(k)$, where k is the winning state of the game. The authors also consider layered games, modelling a system that implements multiple Moving Target Defence techniques, for which the attacker is required to attack one at a time, deriving a similar result to this theorem.

2.1.2 A Game Theoretic Approach to Strategy Determination for Dynamic Platform Defences

This paper models the hacking scenario has a game with in which the attacker has perfect information, whereas the defender does not [11]. At each time interval the system migrates from platform p_i to platform p_{i+1} . The goal of the attack is to compromise platforms $p_i, p_{i+1}, \dots, p_{i+K}$ for some fixed integer K in order to successfully compromise the system. At this point, two variations of the game are considered:

1. The attacker immediately wins the game,
2. The pay-off function of the attacker increases until a critical value is reached.

Two types of attacker are considered. The first is static in nature, in which observing the system gives the attacker no advantage, whereas the adaptive attacker can develop countermeasures for a given platform dependent on the amount of observations made. Five different strategies for platform migration are considered, including randomly selecting platforms from a uniform distribution, from 3 randomly selected prior to the beginning of the trial and selecting the platform least similar to the previous platform according to an equation. Selecting the least similar platform as the migration target has a compromise frequency of only 2%. In contrast, uniform selection eventually results in a 79% compromise rate.

2.1.3 Empirical Game-Theoretic Analysis for Moving Target Defense

This paper models a game with M servers, in which attackers and defenders compete for control of said servers [12]. The paper discusses the possible strategies that can be employed by both the attacker and defender, concluding with details about the Nash equilibria of the games played. Overall, 72 game instances were discovered, with multiple instances of Nash equilibrium, including

Maximal Defense - the defender has such an aversion to attacks that the attacker cannot compromise enough of the system, and gives up.

Maximal Attack - the attacker is so successful at attacking servers that the defender can't do any better than to give up.

Fight - the attacker and defender are both successful at attacking and defending respectively, resulting in constant taking of servers with no win condition being achieved by either party.

Share - the attacker and defender achieve their win conditions simultaneously, and no longer attempt to take servers from the other party.

2.2 Evolutionary Models

2.2.1 Evolutionary Based Moving Target Cyber Defense

This paper discusses two genetic algorithms for producing a Moving Target Defence system, differing by mutation process [13]. The first algorithm mutates the values of

parameters, whilst the other will mutate the domain of a parameter. Each algorithm consists of 140 chromosomes in each generation, where each chromosome is a composition of 102 parameters. Selection of the mutations was done uniformly with 0.25 probability, and via two-round tournament selection with 75% probability. The authors recommend further work to this selection processes as an improvement to the model.

Chapter 3

Aims & Objectives

There are two primary aims to this project. The first aim is the construction of a suitable game-theoretic model for an attack-defence scenario with energy considerations. The second aim is to simulate such a scenario computationally and gather data related to the predictions made by the model. The game theoretical model will be inspired by research, some discussed in the previous chapter. The simulation will test this new model against a genetic algorithm, inspired by previous research, to determine viability for energy reduction of both models.

3.1 Mathematical Modelling

3.1.1 Choice of Moving Target Defences

The structure of Moving Target Defence techniques can vary, consequently the models are prone to variation. Particular techniques will be selected, but any generalisation that can occur will be done.

3.1.2 Threat Model

A suitable threat model will need to be designed. Behaviours of the attacker will be based on how the system is modelled and will inform the strategies that each party will employ.

3.1.3 Modelling Energy Usage

When modelling energy usage, consideration of all forms of energy consumption will need to be made. While the goals of minimising this energy might differ between different instances of Moving Target Defence, such as minimising power for local machines or minimising server usage for cloud platforms, these should all be reflected in the energy usage.

3.2 Experimental Simulation

3.2.1 Genetic Algorithms

Due to the nature of genetic algorithms, it is unlikely that they can be adequately modelled mathematically in a similar fashion to the game theoretical models. As such, experimental simulations will be conducted as a means of comparing these techniques. Research has been conducted into the development of such algorithms [14–17].

3.2.2 Benchmarks

The first benchmark which the genetic algorithm is to be compared to is the properties of the game theoretical model. This allows the algorithm to be compared for defence performance and for energy consumption. Genetic algorithms from the literature can also be used as benchmarks; these were discussed in 3.2.1. Evaluation techniques for Moving Target Defence systems have been developed, and their use in evaluating the techniques developed in this project is likely [13, 18].

Chapter 4

Research Methods

This chapter discusses the philosophies and methods that will be employed to conduct this research project. The reliability of the results is then discussed, along with risk and limitations to the project and the steps taken to avoid their impact.

4.1 Philosophies & Strategies

The research into the mathematical model is deductive, in that properties of the model are deduced from its axioms, assumptions and previous research. Positivism is the philosophical basis for the experiment comparing genetic algorithms with the derived models. This research project will have two main units of analysis. The first being the developed model of a Moving Target Defence system and the second being the computer simulation that models the system. Game Theory is a highly developed mathematical theory on which the model will be based. A model is constructed, informed by a literature review of existing models, and the properties of the constructed model are deduced via mathematical logic. The simulation is experimental in nature.

4.2 Data Collection & Evaluation Methods

No data will be collected from the mathematical model. Rather, properties of the model will be deduced. This will be compared to quantitative data collected from the simulation of the system. Quantities, such as the time until a successful hack and the proportion of successful hacks in a sample of hack attempts, will be outputs of the simulation. These will be treated with a frequentist approach, and hypothesis testing will be used to compare to the values obtained from other models.

4.3 Reliability and Validity

The validity of the model is deduced from the results of the devised experiments. The experiments will be repeated a large number of times to guarantee validity of the results. It is worth mentioning that the results will only truly reflect the models being discussed. Their application to real Moving Target Defence systems, however, is more tenuous and can only be justified by the original assumptions and axioms used. This justification, and any experiments with real systems is outside the scope of this project.

4.4 Risks & Limitations

Multiple risks exist that can compromise the success of this project. The most apparent risk is the time limitation due to work obligations to the DVLA. Coupled with this is the possibility of poor time management: having work priorities for 4 working days requires the rest of the week to be managed carefully. As such, a Gantt chart, figure [5.1](#) has been developed to roughly outline the progress required by each date in order to successfully complete the project.

Chapter 5

Resources & Planning

This section discusses the resources required to complete the research project and presents a Gantt chart that evidences a project plan.

5.1 Resources Required

Only a limited number of resources are needed for this project. These are listed below.

1. Computer - to run the simulation software.
2. MATLAB - the environment in which the simulation is run.

5.2 Gantt Chart

A Gantt chart has been created to manage the time-scale of this project. This is a linear project, and this is reflected in the chart. The project has been divided into three sections:

1. Construction of model for hacking scenario.
2. Simulation of hacking scenario.
3. Revision and refinement of simulation and model.

Implicitly, the writing of the thesis is constant throughout the lifetime of the project.

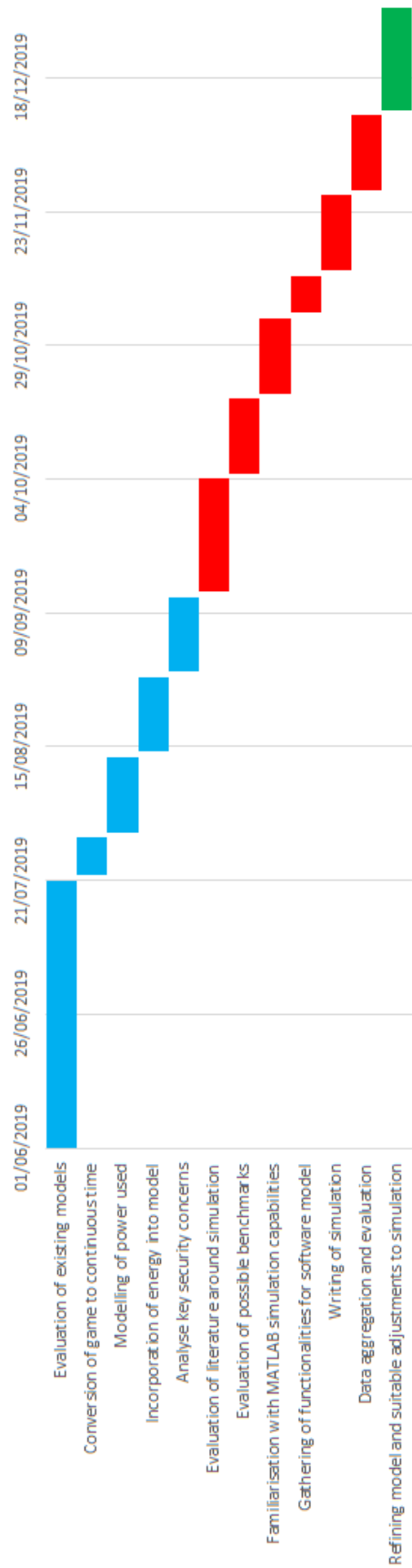


FIGURE 5.1: Gantt chart for the proposed project

Chapter 6

Conclusion

This project aims to analyse models for energy consumption in Moving Target Defence systems. These models are constructed using either game theory or genetic models, which are compared via an experiment. The hope is that research like this, and any subsequent research, will make Moving Target Defence a viable option for defending systems without expending copious amounts of resources.

Bibliography

- [1] L. Marinos, A. Belmonte, and E. Rekleitis, “ENISA threat landscape 2015,” ENISA, Tech. Rep., Jan 2016, accessed: 27/05/2019. [Online]. Available: <https://www.enisa.europa.eu/publications/etl2015/>
- [2] F. Howard, “A closer look at the angler exploit kit,” Sophos Group plc, Tech. Rep., July 2015, accessed: 27/05/2019. [Online]. Available: <https://news.sophos.com/en-us/2015/07/21/a-closer-look-at-the-angler-exploit-kit/>
- [3] N. Biasini, “Threat spotlight: Cisco Talos thwarts access to massive international exploit kit generating \$60m annually from ransomware alone,” Cisco Talos Intelligence Group, Tech. Rep., Oct 2015, accessed: 27/05/2019. [Online]. Available: <https://www.talosintelligence.com/angler-exposed>
- [4] C. Systems Inc., “Cisco 2015 midyear security report,” Tech. Rep., 2015, accessed: 27/05/2019. [Online]. Available: https://www.cisco.com/c/dam/assets/global/UK/events/switchup_challenge/pdf/cisco-msr-2015.pdf
- [5] M. Hopkins and A. Dehghantanha, “Exploit kits: The production line of the cybercrime economy?” *CoRR*, vol. abs/1707.04714, 2017, accessed: 27/05/2019. [Online]. Available: <http://doi.org/10.1109/InfoSec.2015.7435501>
- [6] S. Jajodia and K. Sun, “MTD 2014: First ACM workshop on moving target defense,” in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’14, 2014, pp. 1550–1551.
- [7] NITRD, “National cyber leap year summit 2009 co-chairs’ report,” National Office for the Federal Networking and Information Technology Research and Development Program, Tech. Rep., Sept 2009, accessed: 27/05/2019. [Online]. Available: https://www.nitrd.gov/nitrdgroups/images/b/bd/National_Cyber_Leap_Year_Summit_2009_CoChairs_Report.pdf
- [8] B. Ward, S. Gomez, R. Skowrya, D. Bigelow, J. Martin, J. Landry, and H. Okhravi, “Survey of cyber moving targets,” Massachusetts Institute of Technology, Lexington, Massachusetts, Tech. Rep., Jan 2018.

- [9] P. McDaniel, T. Jaeger, T. F. La Porta, N. Papernot, R. J. Walls, A. Kott, L. Marvel, A. Swami, P. Mohapatra, S. V. Krishnamurthy, and I. Neamtiu, “Security and science of agility,” in *Proceedings of the First ACM Workshop on Moving Target Defense*, ser. MTD ’14, 2014, pp. 13–19.
- [10] H. Maleki, S. Valizadeh, W. Koch, A. Bestavros, and M. van Dijk, “Markov modeling of moving target defense games,” in *Proceedings of the 2016 ACM Workshop on Moving Target Defense*, ser. MTD ’16, 2016, pp. 81–92.
- [11] K. M. Carter, J. F. Riordan, and H. Okhravi, “A game theoretic approach to strategy determination for dynamic platform defenses,” in *Proceedings of the First ACM Workshop on Moving Target Defense*, ser. MTD ’14, 2014, pp. 21–30.
- [12] A. Prakash and M. P. Wellman, “Empirical game-theoretic analysis for moving target defense,” in *Proceedings of the Second ACM Workshop on Moving Target Defense*, ser. MTD ’15, 2015, pp. 57–65.
- [13] D. J. John, R. W. Smith, W. H. Turkett, D. A. Cañas, and E. W. Fulp, “Evolutionary based moving target cyber defense,” in *Proceedings of the Companion Publication of the 2014 Annual Conference on Genetic and Evolutionary Computation*, ser. GECCO Comp ’14, 2014, pp. 1261–1268.
- [14] C. Oehmen, E. Peterson, and S. Dowson, “An organic model for detecting cyber-events,” in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, ser. CSIIRW ’10, 2010, pp. 66:1–66:4.
- [15] C. Oehmen, E. Peterson, and J. Teuton, “Evolutionary drift models for moving target defense,” in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, ser. CSIIRW ’13, 2013, pp. 37:1–37:4.
- [16] A. Makanju, A. N. Zincir-Heywood, and S. Kiyomoto, “On evolutionary computation for moving target defense in software defined networks,” in *Proceedings of the Genetic and Evolutionary Computation Conference Companion*, ser. GECCO ’17, 2017, pp. 287–288.
- [17] S. Wang, L. Zhang, and C. Tang, “A new dynamic address solution for moving target defense,” in *2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference*, May 2016, pp. 1149–1152.
- [18] W. K. Kyi Oo, H. Koide, D. Vasconcellos Vargas, and K. Sakurai, “A new design for evaluating moving target defense system,” in *2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW)*, Nov 2018, pp. 561–563.