Overview of Control and Game Theory in Adaptive Cyber Defenses

George Cybenko[1(✉)], Michael Wellman[2], Peng Liu[3], and Minghui Zhu[3]

[1] Dartmouth, Hanover, USA
gvc@dartmouth.edu
[2] University of Michigan, Michigan, USA
[3] Pennsylvania State University, University Park, USA

Abstract. The purpose of this chapter is to introduce cyber security researchers to key concepts in modern control and game theory that are relevant to Moving Target Defenses and Adaptive Cyber Defense. We begin by observing that there are fundamental differences between control models and game models that are important for security practitioners to understand. Those differences will be illustrated through simple but realistic cyber operations scenarios, especially with respect to the types and amounts of data require for modeling. In addition to modeling differences, there are a variety of ways to think about what constitutes a "solution." Moreover, there are significant differences in the computational and information requirements to compute solutions for various types of Adaptive Cyber Defense problems. This material is presented in the context of the advances documented in this book, the various chapters of which describe advances made in the 2012 ARO ACD MURI.

Keywords: Control Theory · Game Theory · Adaptive Cyber Defense · Moving Target Defense · Autonomous Cyber Operations

1 Moving Target Defenses (MTD)

The computer systems, software applications, and network technologies that we use today were developed in user and operator contexts that greatly valued standardization, predictability, and availability. Even today, performance and cost-effectiveness remain dominant market drivers. It is only relatively recently that security and resilience (not to be confused with fault tolerance) have become equally desirable properties of cyber systems. As a result, the first generation of cyber security technologies were largely based on system hardening through improved software security engineering [7,21] (to reduce vulnerabilities and attack surfaces) and layering security through defense-in-depth [28,31] (by adding encryption, access controls, firewalls, intrusion detection systems, and malware scanners, for example). These security technologies sought to respect the homogeneity, standardization, and predictability that have been so valued by the market but at the same time increasing security.

S. Jajodia et al. (Eds.): Adaptive Cyber Defense, LNCS 11830, pp. 1–11, 2019.
https://doi.org/10.1007/978-3-030-30719-6_1

Consequently, most of our cyber defenses remain static today. They are governed by slow and deliberative processes such as software testing [40], episodic penetration testing [39], security patch deployment [32], and human-in-the-loop monitoring and analysis of security events [12,24,36].

Adversaries benefit greatly from this situation because they can continuously and systematically probe targeted systems with the confidence that those systems will change slowly if at all. Adversaries can afford the time to engineer reliable exploits and pre-plan their attacks because their targets are essentially fixed and almost identical. Moreover, once an attack succeeds, adversaries persist for long times inside compromised networks and hosts because the hosts, networks, and services – largely designed for availability and homogeneity – do not reconfigure, adapt or regenerate except in deterministic ways to support maintenance and uptime requirements. This creates serious information and opportunity asymmetry between IT system defenders and potential attackers [6].

In response to this situation, researchers in recent years have started to investigate a variety of technologies that can make networked information systems less homogeneous and less predictable. Among the terms and concepts used to describe such cyber defense technologies are:

- *Diversity*: Inspired by biological systems [23], cyber diversity is a general concept for introducing robustness and resilience into engineered systems by reducing common failure modes in redundant system components. That is, the goal is to avoid technology "monocultures" [44,53]. In cyber security systems, this is typically accomplished by introducing software or network variants appropriately [10,16,19,30].
- *Randomization*: One approach to introduce cyber diversity is to randomize specific components of an information system. Such randomization can be done at the low level of a system's address space to defeat certain types of memory-based exploits [43], at the software level by generating multiple software variants through compiler randomization [30], instruction set randomization to defeat injected malware [9], or randomization of a network's address space [26] or protocols [33], to give just a few examples.
- *Moving Target Defenses*: Motivated by the observation that a moving target is harder to hit than a fixed one, the general concept behind Moving Target Defenses in the cyber domain is that an information system that changes dynamically *during its operation* will be more difficult for an attacker to surveil, reverse engineer and ultimately exploit with sufficient degrees of persistence than a fixed target [27]. Randomization and diversity are two ways to implement moving target defenses but not all randomization and diversity techniques necessarily realize moving targets. That is because some implementations of diversity and randomization do not in fact change during execution or system recovery after an attack.

A basic goal of Moving Target techniques is to engineer systems that have homogeneous functionalities but dynamically different manifestations. Homogeneous functionality allows authorized use of networks and services in predictable, standardized ways while randomized manifestations make it difficult for attackers to

engineer exploits remotely, let alone parlay one exploit into successful attacks against a multiplicity of hosts or even the same host after reboot. Ideally, each compromise of a system deploying a Moving Target Defense would require the same, significant effort by the attacker who is exploiting the system component in which the Moving Target Defense is deployed.

Although functionality is preserved, it should be noted that there are intrinsic and important tradeoffs between increased security through such means and increased maintenance overhead for managing systems that are less predicable and heterogeneous. Moreover, there are also tradeoffs among the classical security properties of Confidentiality, Integrity and Availability (CIA) when deploying some forms of diversity [20]. For example, having N different and diverse web servers mirroring the same content can increase availability because an attacker has to bring down all N variants, presumably requiring a workfactor about N times higher than bringing down any one web server. On the other hand, the N variants make for a larger attack surface because a breach of any of one of them can compromise confidentiality.

This is but one example of the kinds of tradeoffs that arise when deploying diverse moving targets in an operational environment, namely the possible tradeoffs among security properties valued in the deployment.

In fact, virtually all techniques for increasing security through diversity, randomization and/or moving target defenses involve parameter choices both as individual standalone techniques and especially so when used in combinations [5,17,38,52].

Good or optimal choices for such parameter settings requires modeling the problem, quantifying the model with realistic data and ultimately "solving" the resulting optimization problem. Because the operating environment, mission objectives, mission priorities, attacker behaviors and attacker objectives can all change over time, in fact during exection, moving target deployment solutions might have to be constantly recomputed.

These aspects of Moving Target Defense are the subject of "Adaptive Cyber Defenses" technology addressed in the chapters of this book, and explained in more detail in the following section.

2 Adaptive Cyber Defense: Control and Game Theory for MTD

Research and development in Moving Target Defense has been significant over the past few years.

A 2016 survey paper documented at least 100 different types of Moving Target Defense techniques [14], indicating a significant growth in the number of techniques compared to a 2013 survey [37] that documented 59 different types of Moving Target Defenses. In fact, the development of individual Moving Target Defense Techniques continues at a significant pace today according to a 2018 update to the 2013 survey article [48]. Research on new techniques continues today [2].

The variety of Moving Target Defense techniques together with the variety of options and parameter settings for deploying each individual technique means that there are several types of decisions that an information system operator needs to make to effectively use such techniques. Those decisions include:

- Decisions about which single or combination of MTD's to use;
- Decisions about which MTD parameter settings to use for an individual technique;
- Decisions about which combination of MTD's together with their parameter settings to use (deciding about both of the above simultaneously).

Such decisions are made when MTD's are first deployed and then should be continuously reassessed and updated during deployment seeing as operating and threat conditions change over time. These choices constitute the decision making aspect of the "MTD OODA" (Observe-Orient-Decide-Act) Loop [8,13]. The study of such decisions within the context of MTD's is called Adaptive Cyber Defense (ACD) - the topic of this book.

The rigorous, analytic framework for ACD, namely studying the decision problems arising in MTD-based systems falls within the general scope of Operations Research [51] but more specifically Control Theory and Game Theory. The decision problems are especially challenging when there is inherent uncertainty in the decision-making's operating environment as is typically the case in cyber operations.

The key distinction between Control Theory and Game Theory is the nature of the operating environment and how it is modeled. To illustrate the fundamental difference, consider the following simple but representative MTD cyber defense situation.

In a cloud computing environment, performance of servers and applications degrade over time (due to memory leaks or other inadequate memory management among other reasons, for example). Given availability requirements (such as the average or minimal number of servers available over time) and historical data on performance degradation, it is possible to quantitatively formulate a decision problem regarding schedules for regenerating individual server software. Two fundamentally different modeling frameworks in this scenario are briefly described and compared below.

2.1 Control Theory Models

In this modeling approach, there is a benefit for each time unit that a server is up and fulfilling requests at various rates and there is a time cost for restarting the server with a fresh image. For simplicity of exposition, assume that the server is either working properly or not. During restarts, no requests can be fulfilled because the server is not working. Moreover, there is a probability distribution for the time that the server will fail after a restart. That probability distribution, as well as the value of server uptime and time to restart, are independent of how many restarts have occured and when they occured. Note that if the system is not memoryless, the system operator can be inclined to restart a system even

before it fails outright because the cost of downtime is higher than the cost of restarting. This kind of model is common within the cloud server reliability research literature and can be formulated as a control problem [11,29].

A key aspect of this formulation of the problem is that the operating environment in which the system operates is *non-adversarial* in that the failures are random and independent of each other.

Moreover, control theoretic formulations typically involve computing minima or maxima of objective functions so that the models can be solved using optimization techniques such as dynamic programming.

2.2 Game Theory Models

In the game theory modeling approach, the same costs and benefits for correct server operation hold as in the above control theory model. However, the server failures are no longer solely the result of natural, benign operation but are influenced or even explicitly triggered by rational adversaries (the attackers) who have their own costs and benefits for bringing a server down. The attacker accrues benefit when the server is down but has a cost for launching an attack, successful or not, because some effort is required to exploit a novel vulnerability or to use a new source IP address that is not black-listed.

A key aspect of the game theory formulation of the problem is that the operating environment in which the system operates is decidedly *adversarial* in that the system failures are due to the actions of a rational agent whose objectives are typically at odds with the system operator's objective. As in the above control theory formulation, the system operator can benefit from restarting a system even before it is fulling compromised in an attack because the cost of downtime is higher than the cost of restarting.

The concept of solution to a game theoretic formulation of a problem is typically expressed in terms of equilibria, such as Nash Equilibia. By contrast with control problems, equilibria in games are typically saddle points in the sense that they are maxima for one player and minima for another player.

Such game theory-based models can lead to complex analyses in which there are several open problems [34,46,50].

In both control and game theory, the term "policy" refers to the actions the operator takes to change system states (for example, a "restart" action will take the system from the "failed" state to the "normal operation" state for the operator but for an attacker, the "attack" action will take the targeted system from the "normal" state to the "failed" state. Given an objective function and a concept for a "solution" with respect to that objective function, an optimal policy for each actor is a policy that achieves optimal performance for them with respect to their concept of solution and their objective function.

In this context, Adaptive Cyber Defense (ACD) is the application of control and game theory to Moving Target Defenses (MTD). Notwithstanding the above distinctions, both control and game theory as used in Adaptive Cyber Defense involve many common ingredients. We list the ingredients below along with brief descriptions of them as well as pointers to the literature, including chapters in this book, with detailed approaches (Table 1).

Table 1. Adaptive Cyber Defense (ACD) ingredients

Ingredient	Description	Book chapters	Other references
Moving Target Defense Techniques	Adaptive Cyber Defenses involve the deliberate and rational actions that an operator can invoke to protect their systems. Specific actions considered include possible network, operating systems and applications randomizations, diversity and Moving Target Defenses. Possible actions include configuration and parameter selections for individual techniques. In its totality, this is an enormous action space that no enterprise would consider deploying altogether so it is more realistic to consider these techniques individually or in small combinations only	Chapter 7 [15] Chapter 8 [3]	
Moving Target Defense Quantification	In order to effectively use Moving Target Defenses through the application of control and/or game theory, it is necessary to quantify the methods, their effects, their costs as well as the situation picture the operating environment in which they operate. A variety of efforts have investigated both empirical and analytic techniques for such quantifications	Chapter 5 [1] Chapter 10 [42]	[18,22,41,47]
Adaptive Cyber Defense Control Models and Techniques	Decisions about MTD deployment and operation that are made under worst-case and/or stationary operating conditions are typically modeled as control problems and therefore solvable by control techniques	Chapter 2 [35] Chapter 4 [25] Chapter 8 [3] Chapter 9 [4]	
Adaptive Cyber Defense Game Models and Techniques	Decisions about MTD deployment and operation that are made under operating conditions that are adversarial are typically modeled as game problems and therefore solvable by techniques used for solving game models	Chapter 3 [45] Chapter 6 [49]	[54]

3 Chapter Summaries

Chapter 1 - Overview of Control and Game Theory in Adaptive Cyber Defenses. This chapter is an introduction and overview of the structure and motivation for this book.
Chapter 2 - Control-Theoretic Approaches to Cyber Security. This chapter reviews control theoretic formulations of cyber security problems, focusing on state-based approaches and modeling of uncertainty.
Chapter 3 - Game-Theoretic Approaches to Cyber Security. This chapter reviews game theoretic formulations of cyber security problems, focusing on stochastic dynamic games and modeling of asymmetric information in such games.
Chapter 4 - Reinforcement Learning in Adaptive Cyber Defense. This chapter presents reinforcement learning approaches to solving certain control theoretic formulations of zero-day attack situations.
Chapter 5 - Moving Target Defense Quantification. In order to build and solve either control or game theoretic formulations of cyber security problems, it is necessary to quantify various aspects of the attack/defend engagement. This chapter presents a novel approach to such quantifications.
Chapter 6 - Empirical Game-Theoretic Methods. Empirical game theory does not start with a stylized .abstract model of an adversarial encounter, using simulations of such encounters to create increasingly more complex and accurate models and solutions to the underlying game.
Chapter 7 - Adaptive Cyber Defense Techniques for Memory Protection. This chapter describes several memory corruption cyber attacks and develops dynamic adaptive address space layout randomization (ASLR) approaches to defend against novel attacks.
Chapter 8 - Adaptive Cyber Defense Techniques for Botnet Detection and Mitigation. This chapter describes the botnet detection and mitigation problems together with adaptive cyber defense approaches to solving them using both control and game theoretic formulations.
Chapter 9 - Optimizing Alert Management Processes in Cyber Security. This chapter describes the cyber security alert management problem together with control theory based approaches to optimizing tasks and personnel assignments in Cyber Security Operations Centers (CSOC).
Chapter 10 - Online and Scalable Adaptive Cyber Security Defense. This chapter decribes problems related to the online state and parameter estimation and approximation required in certain adaptive defense techniques. The focus is on using recently developed so-called "sketching" techniques that allow approximating various structural and statistical properties of data streams using only limited storage and processing time.

Acknowledgements and Disclaimer. The work presented in this book was support by the Army Research Office under grant W911NF-13-1-0421. The authors of this book and other participants in the Adaptive Cyber Defense project are grateful for the direction and support of Dr. Clifford Wang (U.S. Army Research Office).

The views and opinions expressed in this book are those of the authors and do not necessarily reflect the official policy or position of any agency of the U.S. Government.

References

1. Albanese, M., Connell, W., Venkatesan, S., Cybenko, G.: Moving Target Defense Quantification (chap. 5). Springer, New York (2018)
2. Albanese, M., Huang, D.: MTD 2018: 5th ACM workshop on Moving Target Defense (MTD). In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 2175–2176. ACM (2018)
3. Albanese, M., Jajodia, S., Venkatesan, S., Cybenko, G., Nguyen, T.: Adaptive Cyber Defenses for Botnet Detection and Mitigation (chap. 8). Springer, New York (2018)
4. Albanese, M., Jajodia, S., Venkatesan, S., Cybenko, G., Nguyen, T.: Adaptive Cyber Defenses for Botnet Detection and Mitigation (chap. 9). Springer, New York (2018)
5. Anderson, N., Mitchell, R., Chen, R.: Parameterizing moving target defenses. In: 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–6. IEEE (2016)
6. Anderson, R., Moore, T.: The economics of information security. Science **314**(5799), 610–613 (2006)
7. Anderson, R.J.: Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, Hoboken (2010)
8. Angerman, W.S.: Coming full circle with Boyd's OODA loop ideas: an analysis of innovation diffusion and evolution. Technical report, Air Force Inst Of Tech Wright-Patterson AFB OH School of Engineering and Management (2004)
9. Barrantes, E.G., Ackley, D.H., Forrest, S., Stefanović, D.: Randomized instruction set emulation. ACM Trans. Inf. Syst. Secur. (TISSEC) **8**(1), 3–40 (2005)
10. Baudry, B., Monperrus, M.: The multiple facets of software diversity: Recent developments in year 2000 and beyond. ACM Comput. Surv. (CSUR) **48**(1), 16 (2015)
11. Bertsekas, D.P.: Dynamic Programming and Optimal Control, vol. 1. Athena Scientific Belmont, Belmont (2005)
12. Bhatt, S., Manadhata, P.K., Zomlot, L.: The operational role of security information and event management systems. IEEE Secur. Priv. **5**, 35–41 (2014)
13. Boyd, J.R.: The essence of winning and losing. Unpublished lecture notes 12(23), 123–125 (1996)
14. Cai, G.L., Wang, B.S., Hu, W., Wang, T.Z.: Moving target defense: state of the art and characteristics. Front. Inf. Technol. Electron. Eng. **17**(11), 1122–1153 (2016)
15. Chen, P., et al.: MTD Techniques for Memory Protection against Zero-Day Attacks (chap. 7). Springer, New York (2018)
16. Co, M., et al.: Double Helix and RAVEN: a system for cyber fault tolerance and recovery. In: Proceedings of the 11th Annual Cyber and Information Security Research Conference, p. 17. ACM (2016)
17. Collins, M.P.: A cost-based mechanism for evaluating the effectiveness of moving target defenses. In: Grossklags, J., Walrand, J. (eds.) GameSec 2012. LNCS, vol. 7638, pp. 221–233. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34266-0_13

18. Connell, W., Albanese, M., Venkatesan, S.: A framework for moving target defense quantification. In: De Capitani di Vimercati, S., Martinelli, F. (eds.) SEC 2017. IAICT, vol. 502, pp. 124–138. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-58469-0_9
19. Cox, B., et al.: N-variant systems: a secretless framework for security through diversity. In: USENIX Security Symposium, pp. 105–120 (2006)
20. Cybenko, G., Hughes, J.: No free lunch in cyber security. In: Proceedings of the First ACM Workshop on Moving Target Defense, pp. 1–12. ACM (2014)
21. Devanbu, P.T., Stubblebine, S.: Software engineering for security: a roadmap. In: Proceedings of the Conference on the Future of Software Engineering, pp. 227–239. ACM (2000)
22. Farris, K.A., Cybenko, G.: Quantification of moving target cyber defenses. In: Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security, Defense, and Law Enforcement XIV, vol. 9456, p. 94560L. International Society for Optics and Photonics (2015)
23. Forrest, S., Somayaji, A., Ackley, D.H.: Building diverse computer systems. In: The Sixth Workshop on Hot Topics in Operating Systems, pp. 67–72. IEEE (1997)
24. Ganesan, R., Jajodia, S., Cam, H.: Optimal scheduling of cybersecurity analysts for minimizing risk. ACM Trans. Intell. Syst. Technol. (TIST) (TIST) **8**(4), (2017). Article no. 52
25. Hu, Z., Chen, P., Zhu, M., Liu, P.: Reinforcement Learning for Adaptive Cyber Defense against Zero-day Attacks (chap). 4. Springer, New York (2018)
26. Jafarian, J.H., Al-Shaer, E., Duan, Q.: Openflow random host mutation: transparent moving target defense using software defined networking. In: Proceedings of the First Workshop on Hot Topics in Software Defined Networks, pp. 127–132. ACM (2012)
27. Jajodia, S., Ghosh, A.K., Swarup, V., Wang, C., Wang, X.S.: Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats, vol. 54. Springer, Cham (2011)
28. Jajodia, S., Noel, S., Kalapa, P., Albanese, M., Williams, J.: Cauldron mission-centric cyber situational awareness with defense in depth. In: IEEE MILCOM, pp. 1339–1344 (2011)
29. Jung, G., Joshi, K.R., Hiltunen, M.A., Schlichting, R.D., Pu, C.: Performance and availability aware regeneration for cloud based multitier applications. In: 2010 IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 497–506. IEEE (2010)
30. Larsen, P., Homescu, A., Brunthaler, S., Franz, M.: SoK: automated software diversity. In: 2014 IEEE Symposium on Security and Privacy (SP), pp. 276–291. IEEE (2014)
31. Lippmann, R., et al.: Validating and restoring defense in depth using attack graphs. In: IEEE MILCOM, pp. 1–10 (2006)
32. Lippmann, R., Webster, S., Stetson, D.: The effect of identifying vulnerabilities and patching software on the utility of network intrusion detection. In: Wespi, A., Vigna, G., Deri, L. (eds.) RAID 2002. LNCS, vol. 2516, pp. 307–326. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-36084-0_17
33. MacFarland, D.C., Shue, C.A.: The SDN shuffle: creating a moving-target defense using host-based software-defined networking. In: Proceedings of the Second ACM Workshop on Moving Target Defense, pp. 37–41. ACM (2015)
34. Marden, J.R., Shamma, J.S.: Game theory and control. Annu. Rev. Control Robot. Auton. Syst. **1**, 105–134 (2018)

35. Miehling, E., Rasouli, M., Teneketzis, D.: Control-Theoretic Approaches to Dynamic Cyber Security (chap. 2). Springer, New York (2018)
36. Novikova, E., Kotenko, I.: Analytical visualization techniques for security information and event management. In: 2013 21st Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), pp. 519–525. IEEE (2013)
37. Okhravi, H., et al.: Survey of cyber moving target techniques. Techical report, Massachusetts Institute of Technology: Lexington Lincoln Lab (2013)
38. Okhravi, H., Riordan, J., Carter, K.: Quantitative evaluation of dynamic platform techniques as a defensive mechanism. In: Stavrou, A., Bos, H., Portokalidis, G. (eds.) RAID 2014. LNCS, vol. 8688, pp. 405–425. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-11379-1_20
39. Pfleeger, C.P., Pfleeger, S.L., Theofanos, M.F.: A methodology for penetration testing. Comput. Secur. **8**(7), 613–620 (1989)
40. Potter, B., McGraw, G.: Software security testing. IEEE Secur. Priv. **2**(5), 81–85 (2004)
41. Priest, B.W., Vuksani, E., Wagner, N., Tello, B., Carter, K.M., Streilein, W.W.: Agent-based simulation in support of moving target cyber defense technology development and evaluation. In: Proceedings of the 18th Symposium on Communications & Networking, pp. 16–23. Society for Computer Simulation International (2015)
42. Priest, B.W., Cybenko, G., Liu, P., Singh, S., Albanese, M.: Online and Scalable Adaptive Cyber Defense (chap. 10). Springer, New York (2018)
43. Shacham, H., Page, M., Pfaff, B., Goh, E.J., Modadugu, N., Boneh, D.: On the effectiveness of address-space randomization. In: Proceedings of the 11th ACM Conference on Computer and Communications Security, pp. 298–307. ACM (2004)
44. Stamp, M.: Risks Monoculture. Communications of the ACM **47**(3), 120 (2004)
45. Tavafoghi, H., Ouyang, Y., Teneketzis, D., Wellman, M.: Game Theoretic Approaches to Cyber Security: Challenges, Results and Open Problems (chap. 3). Springer, New York (2018)
46. Van Dijk, M., Juels, A., Oprea, A., Rivest, R.L.: Flipit: the game of "stealthy takeover". J. Cryptol. **26**(4), 655–713 (2013)
47. Van Leeuwen, B., Stout, W.M., Urias, V.: Operational cost of deploying moving target defenses defensive work factors. In: Military Communications Conference, MILCOM 2015 – 2015 IEEE, pp. 966–971. IEEE (2015)
48. Ward, B.C., et al.: Survey of cyber moving targets, 2nd edn. Technical report, MIT Lincoln Laboratory Lexington United States (2018)
49. Wellman, M.P., Nguyen, T.H., Wright, M.: Empirical Game-Theoretic Methods for Adaptive Cyber-Defense (chap. 6). Springer, New York (2018)
50. Wellman, M.P., Prakash, A.: Empirical game-theoretic analysis of an adaptive cyber-defense scenario (preliminary report). In: Poovendran, R., Saad, W. (eds.) GameSec 2014. LNCS, vol. 8840, pp. 43–58. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-12601-2_3
51. Winston, W.L., Goldberg, J.B.: Operations Research: Applications and Algorithms, vol. 3. Thomson Brooks/Cole, Belmont (2004)
52. Xu, J., Guo, P., Zhao, M., Erbacher, R.F., Zhu, M., Liu, P.: Comparing different moving target defense techniques. In: Proceedings of the First ACM Workshop on Moving Target Defense, pp. 97–107. ACM (2014)

53. Zhang, M., Wang, L., Jajodia, S., Singhal, A., Albanese, M.: Network diversity: a security metric for evaluating the resilience of networks against zero-day attacks. IEEE Trans. Inf. Forensics Secur. **11**(5), 1071–1086 (2016)
54. Zhu, Q., Başar, T.: Game-theoretic approach to feedback-driven multi-stage moving target defense. In: Das, S.K., Nita-Rotaru, C., Kantarcioglu, M. (eds.) GameSec 2013. LNCS, vol. 8252, pp. 246–263. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-02786-9_15