

Survey on quantitative evaluations of moving target defense

Huanruo LI, Yunfei GUO, Shumin HUO, Guozhen CHENG, Wenyan LIU

National Digital Switching System Engineering & Technological R&D Center Zhengzhou 450002, China

Abstract: Quantitative evaluations are of great importance in network security decision-making. In recent years, moving target defense (MTD) has appeared to be a promising defense approach that blocks asymmetrical advantage of attackers and favors the defender-notwithstanding, it has a limited deployment due to its uncertain efficiency and effectiveness in defense. In that case, quantitative metrics and evaluations of MTD are essential to prove its capability and impulse its further research. This article presents a comprehensive survey on state-of-the-art quantitative evaluations. First, taxonomy of MTD techniques is stated according to the software stack model. Then, a concrete review and comparison on existing quantitative evaluations of MTD is presented. Finally, notice-worthy open issues regarding this topic are proposed along with the conclusions of previous studies.

Key words: quantitative evaluation, moving target defense, security metrics

doi: 10.11959/j.issn.2096-109x.2018076

1 Introduction

Network has become so indispensable in today's globalized world. Diverse network technologies have been researched and developed in profound, which enhance almost every aspect of human life: business, education, finance, medical facility and culture communication, etc. However, major incidents reported recent years (WannaCry, Nyetya, PRISM and Facebook data leakage, etc.) have shown that the huge benefits from network are accompanied with hazardous attacks. Network attack is more like a butterfly effect where even a minor change in the network state can result in severe socio-economic disasters such as great losses on finance, leakage on vital information or even a dilemma in political situation. One of the root causes of the severe circumstances today is that network configurations are mostly static, deterministic and monocultural. This allows malicious internet users

to take advantage and exploit on system vulnerabilities.

Recently, a promising defense approach, moving target defense (MTD) is surfaced. It provides a potential in blocking the asymmetrical advantage of attackers and is in favor of defenders. MTD defends objects through conducting changes on system in multiple dimensions to reduce the attack surfaces and increase the complexity for attackers. This limits the exposure of vulnerabilities, minimizes the probing probabilities and maximizes the cost of attackers.

MTD techniques include shifts and changes overtime in any part of network system^[1]. Despite it's very potential to be widely applied in different level of software stack or network systems, MTD has limited deployment in the real scenario. One of the most essential reasons is that "you cannot compare and improve something that you cannot measure"^[2], without appropriate quantitative evaluation

Received data: 2018-06-10; **Revised data:** 2018-08-10

Corresponding Author: Huanruo LI, viaviavialhr@outlook.com.cn

Foundation Items: The National Natural Science Foundation of China (No.61521003), The National Key R&D Program of China (No.2016YFB0800100, No.2016YFB0800101), The National Natural Science Foundation of China (No.61602509), The Key Technologies Research and Development Program of Henan Province (172102210615)

approaches, we can hardly leverage MTD against existing defense mechanisms in effectiveness and efficiency. Thus, quantitative evaluations and metrics are of great significance.

In this paper, we emphasize the significance of quantitative evaluation of MTD techniques, conclude state-of-the-art evaluation approaches and propose existing challenges for current researches in this field. Furthermore, we compare each MTD techniques (in the same category according to software stack model) and some existing evaluation methods. This paper will serve as a reference towards quantification evaluation and its metrics on MTD. The remainder of the paper is organized as follows: Section II describes the taxonomy/ categories of MTD techniques; Section III depicts challenges and major quantitative evaluations of MTD, along with an abstract of existing security metrics; Section IV proposes and discusses notice-worthy open issues. Finally, Section V offers concluding remarks and future work.

2 Taxonomy of moving target defense techniques

The taxonomy of Moving Target Defense Techniques varies from application scenario-based, dynamic techniques-based to attack model-based. In this paper, we adopt the taxonomy of Moving Target Defense Techniques according to the Survey of cyber moving target^[3], which is categorized based on software stack.

According to software stack model (figure 1), moving target defense techniques can be classified into five different domains: data-based, software-based, runtime environment-based, platform-based and network-based in accordance with their place within the execution stack^[4]. 1) In data-based techniques, data is the moving factors and is dynamically altered in format, syntax and encoding^[3]. Typical techniques, such as data randomization^[5], NOMAD and document content randomiza-

tion (DCR), usually defense system against code injection, control injection, SQL injection and web bots, etc^[6]. 2) In software-based techniques, alternations are mainly in code and its composition^[7]. Dynamic encryption, compilation, execution and modified program instructions are applied so as to perform effective defense^[8]. Mainstream applications are CCFIR: compact control flow integrity and randomization, proactive obfuscation^[9], program differentiation and software diversity using distributed coloring, etc. 3) In runtime environment-based techniques, dynamic changes are performed on the execution environment of certain or all applications so as to realize moving target defense^[3]. Under this classification, there are two sub-categories: address space layout randomization (ASLR) and Instruction-Set Randomization (ISR)^[10]. Representative techniques such as address space layout permutation (ASLP)^[11] and randomized instruction-set emulation (RISE) are deeply researched and widely deployed nowadays. 4) As for platform-based techniques, changes on platform (operating system (OS) or CPU) properties are conducted^[12]. Existed techniques are, for instance, N -variant systems, moving target surface, dynamic application rotation environment for moving target defense and talent, etc. 5) In network-based techniques, changes are performed on network properties such as protocol and address so as to implement dynamic defense on network topology, configuration, resources, nodes and services^[13]. Techniques in this field is well-developed, some typical techniques are: dynamic network address translation (DYNAT)^[14], NASR^[15], random host mutation and resilient overlay networks (RON)^[16], etc.

3 Major quantitative evaluation methods and security metrics on MTD techniques

A good evaluation with appropriate security metrics will enable effective assessment and comparison between MTD and existing defense methods.

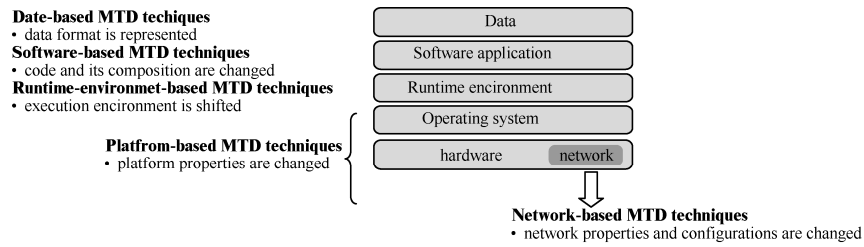


Figure 1 Taxonomy of moving target defense techniques according to software stack model

Table 1 Details of MTD techniques of different categories and implementing mechanisms

Category	MTD Techniques	Mitigation
Data-based	Data Randomization NOMAD Document Content Randomization (DCR)	Code Injection and Control Injection Automated Web Bots Malicious Microsoft Office Documents
Software-based	CCFIR: Compact Control Flow Integrity and Randomization Proactive Obfuscation Program Differentiation Software Diversity Using Distributed Coloring	Control Injection Code Injection and Control Injection Code Injection and Control Injection Code Injection
Runtime Environment-based	Address Space Randomization (ASLR): Address Space Layout Permutation (ASLP) Instruction-Set Randomization (ISR): Randomized Instruction Set Emulation (RISE)	Code Injection and Control Injection Code Injection
Platformed-based	N-Variant Systems Moving Target Surface Dynamic Application Rotation Environment for Moving Target Defense TALENT	Code Injection and Control Injection Code Injection, Control Injection and Scanning Code Injection, Control Injection and Scanning Code Injection, Control Injection, Scanning, Supply Chain
Network-based	DYNAT NASR Random Host Mutation Resilient Overlay Networks (RON)	Resource, Spoofing, Data Leakage Resource and Scanning Scanning Resource, Spoofing, Data Leakage

Also, it provides evidence and reference for future configuration and development. Many researches have been done in evaluating network defense, including empirical and quantitative methods, but few focuses on MTD. As for security metrics, lockheed martin kill chain^[17] and Common Vulnerability Scoring System^[18-21], for instance, can be applied in general defense evaluation methods, while some other metrics are designed for specified methods.

In this section, we will bring up some challenges of evaluating MTD and concentrate on quantitative evaluations of MTD. First, we will describe existing challenges on evaluating and assessing MTD techniques, which will be further discussed in conclusion section IV. In the following, a rough study on typical techniques of MTD for each category will be presented along with their evaluation methods. The introduction of quantitative evaluation

may include certain description of metrics so as to have a deeper understanding. In the end, we will draw a summary and comparison among all evaluations.

The challenges of evaluating MTD techniques: 1) Overlooking on overheads. Taking overheads into consideration is complicated but necessary. Most existing models consider only the effectiveness of defense while the deployment overheads are left behind. However, an efficient defense approach could strike a balance between cost and effectiveness. 2) The lack of quantitative evaluation approaches. A lot of existing evaluation methods are empirical-based, which are not so precise and appropriate to evaluate MTD techniques and instruct on further researches. 3) Effectiveness identification. A certain technique are composed of different parts, also, network defense requires different techniques

deployed altogether to reach the best result. A lot of researches indicate the potential of multi-deploying MTD techniques but it remains to be verified. Because there lacks an evaluation model or method that can identify the most effective part of the technique or the effectiveness of layer-deployed techniques. 4) The lack of effective and generalized quantitative metric, attacking models and testbeds. Most existing evaluation methods aim at one or a specific type of defense. Without a generalized evaluation, different techniques can't be compared with each other under same criteria.

3.1 Evaluation on data-based MTD techniques

In[22], Nguyentuong et al. propose redundant data diversity and evaluate the variation through a case study in Apache Http Server, making use of the only one complicating factor Apache has. The detailed evaluation process is that they created Apache variants through changing source code and analysis the information in error messages Apache ever encountered. From the amount and content of error messages, authors conclude the effectiveness of this technique. However, detailed quantitative metrics are not demonstrated. The result of the case study shows quantification effectiveness of redundant data diversity as well as its implementation overheads.

In[5], Cadar et al. propose a series of experiments to evaluate the effectiveness of data randomization including its deployment overheads and its effectiveness of preventing attacks. In the experiment of measuring overheads, they compare the running time and peak physical memory usage of the programs compiled with and without implementing data randomization. The result shows that there are overheads increase in a scale but acceptable. When it comes to the effectiveness of preventing attacks, they adopt a benchmark with synthetic exploits and several exposed vulnerabilities in existing programs. The benchmark they adopt contains 18 control-data attacks under the category of direct overwrite on stack, data segment and through stack

pointer and data segment pointer. These attacks exploit buffer overflow vulnerabilities. Additionally, they adopt a set of real vulnerabilities in SQL server, Ghttpd, Nullhttpd and Stunnel so as for a final test (the scale of being exploited is adopted to make comparison) for the effectiveness of data randomization. Compared with the defense performance, the overheads are quite low according to their experiment results. This method allows us to have a direct understanding of the effectiveness of data randomization through showing exploits. It can also be applied in evaluating the other data-based MTD techniques.

In[23], Smutz et al. propose Document Content Randomization technique that mitigates some attacks on documents and prevents hosts from being attacked by malicious documents with randomizing data block order and modify some Microsoft files. The evaluation concentrates on the number of software vulnerabilities that malicious documents leverage. This technique is designed to put in practice, so the authors assess DCR in real attack scenario with documents from VirusTotal and the number of exploits being blocked indicates the capability and effectiveness of DCR. The advantage of this evaluation is that: it is more practical and intuitive to be accepted.

In[24], Vikram et al. propose NOMAD, a non-intrusive moving target defense against web bots. They evaluate NOMAD with deploying it on forum and blogging instances (ohoBB, SMF, WordPress and BuddyPress) without a typical model. Web bots: XRunmer, MagicSubmitter, UWCS, Comment Blaster and SENUke are adopted to perform simulations. In this evaluation, attack results (success or failure) is regarded as the metric and overhead is evaluated by page loading time and page size. The advantage of this evaluation is that overheads and costs are included and considered as a whole proving the efficiency of NOMAD. Also, the attack experiment intuitively indicates the effec-

tiveness. However, this evaluation method does not satisfy universality and doesn't produce a quantification metrics.

Summary: With studying data-based MTD techniques, we find out that test-based quantitative evaluations are often applied^[5,22-26], it is notice worthy that evaluation proposed in [23] is practiced under real scenario. Some other evaluation methods adopt empirical benchmarks such as those in [26]. The results of the above evaluations are presented in quantitative way and the differences lie in [22-23] propose detailed quantitative metrics, evaluate both efficiency and effectiveness but lack of universality in widely apply^[5]; is evaluated with real vulnerabilities but measure with empirical benchmark and also lacks universality in application. In general, quantitative evaluation, especially test or experiment-based ones, are widely adopted in data-based MTD techniques. For fulfilling the challenge of evaluating MTD techniques, most of these methods use quantitative security metrics, concern on both effectiveness and efficiency of defense and give a quantitative result. The existing demerits are lack of universal evaluation metrics or standard for a wider evaluation scenario.

3.2 Evaluation on software-based and runtime environment-based MTD techniques

In [27], Koning et al. propose MvArmor, a multi-variant eXecution (MVX) system provides thorough protection against memory error exploits. MvArmor is evaluated with simulation-based approaches. The overheads are tested with SPEC CINT 2006. The security effectiveness is evaluated with deploying some real-world vulnerabilities. The security metrics lie in the disclosure of data and information. The merit of this evaluation method is that it can be applied to evaluate the other software-based MTD techniques.

In [28], Crane et al. propose a dynamic software-based technique to defense side-channel attacks. This technique is providing probabilistic de-

fense on both online and offline side-channel attacks with diversifying and randomizing control flow of programs. An evaluation approach is offered applying modification of synchronous known-data attacks^[29] and asynchronous attacks are implemented into attacking scenario. Empirical methods are adopted to analyze the compromised rate and generate the results. And AES Micro-benchmark is adopted to measure the cost.

Runtime environment-based MTD techniques are classified into Address Space Randomization and Instruction-Set Randomization. In [30], Evans et al. propose a model to evaluate MTD techniques especially runtime environment-based and data-based ones. Their model is consisted of two layers: an attacker and a defender. As for the attacker, five different attack strategies have been introduced: circumvention attacks, deputy attacks, brute force and entropy reduction attacks, probing attacks and incremental attacks. They analyze and quantify the probability of a successful attack with attackers adopting one or more of the five strategies on an MTD-deployed system. The effectiveness of Runtime time-based MTD techniques are determined by the probability of a successful attack and probability without re-randomization. The advantage of this method is that the model-based probabilities reveal the effectiveness of MTD techniques and simulate with real attack strategies. Also, they figure out the factors and configurations to improve for a better defense system. However, this is an empirical model which lacks quantified outputs to illustrate effectiveness. And the evaluation is conducted on a single diversity defense, that is, ALSR and ISR are evaluated separately, the effectiveness of a layer-deployed application is not verified yet.

Summary: In evaluating software-based and runtime environment-based MTD techniques, there are simulation-based^[27], model-based and attack-model-based^[28-29] quantitative methods. To

answer the challenges on evaluating MTD techniques, method in [27] achieves universality that can be used in quantitatively evaluating other software-based MTD but the balance-striking between effectiveness and efficiency is neglected. While that in [28] is based on empirical evaluation and not supportive enough for further investigation. The model-based approach proposed in [30] can be used in both software-based and runtime environment-based MTD techniques, this model is very thorough but it fails to provide quantitative metrics and results. Also effectiveness identification remains to be researched.

3.3 Evaluation on platform-based MTD techniques

In [31], Okhravi et al. study the features of existed platform-based MTD techniques, measure the protection provided by them and quantify the effectiveness with generating a universally applicable evaluating model. They take Talent^[32] for instance and conduct an experiment to evaluate major effect of dynamic platform techniques on system security. With abstracting the knowledge and results from the experiment, they propose a generalized model. Their evaluation includes a threat model, two real exploits against Talent (TCP MAXSEG and socket pairs) and a pool with platforms. Each platform will be selected in each configuration randomly. They conclude five effects that impact on the results which are limited duration, diversity, multi-instance, cleanup and smoothing, which could be deemed as the metric they apply into evaluating. The effectiveness of dynamic platform techniques (DPT) is depicted in the time (attackers take) to disrupt the service and success rate. The quantification model they propose include attacker aggregate control model, attacker continuous control model, attacker fractional payoff model and attacker binary payoff according to different situation and aspects. Furthermore, they verify major effects of DPT on system security and their generalized model through

simulations. In general, this is a thorough model-based quantitative evaluation with detailed metrics and algorithm that depict the model and reach a quantitative evaluation result. Also, it is notice worthy that authors have mentioned that the measurement and metric of effectiveness should take threat model into consideration.

In [33], Cai et al. propose a generalized model to evaluation MTD techniques. As it is stated, this model applies to not only DPT but also Software Transformation and Network Address Shuffling. Random Host Mutation is taken for case study. Cai's model is based on generalized stochastic petri net (GSPN)^[33]. Five different switches are provided as to measure the effectiveness of maneuver. Moreover, time delay will be taken into consideration and calculates with token. In final, a self-defined parameter will be calculated by the GSPN-based evaluator as a reference on the effectiveness of corresponding techniques. The advantage of this model is that it can be applied to three typical MTD techniques and generate concrete quantification result with a model.

In [34], Anderson et al. propose two analytical models for evaluating and assessing the effectiveness of platform-based MTD techniques. Their models are inspired by closed form solutions and stochastic petri nets (SPN). Closed-form model is applied to calculate the success rate of an attack on the scenarios implemented MTD techniques. And the SPN is used to describe the cyber engagement ecosystem. Markov is used within this model to calculate the probability of attack success rate, which also is the reflection on the effectiveness of DPT. According to this work, the two model they provided are computational efficiency. The advantage of this model is that they experiment with some lasting attacks and quantify attacks with success rate and evaluate the effectiveness of platform-based techniques with the same results.

Summary: In studying platform-based MTD techniques, we find out that mainstream evaluations

are based on model and simulation. To address the challenges in evaluating MTD techniques^[31, 33, 35], all proposed thorough quantitative models. Their improvements lie in the application of mathematical models and applicable for almost all platform-based techniques. But the applicable range is quite small^[33, 35] and the overheads are neglected in the model^[35]. Furthermore, few researches on defense applying techniques of multiple categories has been done here, the effectiveness identification issue is not well addressed yet.

3.4 Evaluation on network-based MTD techniques

In [36], Collins et al. propose an evaluation on network-based MTD techniques applying tag switching. The design of tag switching breaks network into tags and assets. The connection between tags and assets are internet protocols. The core of this model is that it evaluates certain or general techniques with tag space, which not only describes tags and assets, but also quantifies the attacker's ability. By manipulating tag/asset relationship, defense techniques' impact on network system are countable to determine the defensive performance and effectiveness.

In [37], Hong et al. propose hierarchical attack representation model (HARM), which is a 2-layer model, to assess the effectiveness of an MTD technique. Their proposal takes formal security models into consideration (attack graph (AG) or attack tree (AT)). HARM evaluation method will be more scalable and adaptable. In the statement, they first classify MTD techniques into shuffle, diversity and redundancy. And then they evaluate certain techniques with the 2-layer HARM model, including the upper layer deploying AG and the lower layer deploying AT. They conduct simulations on verifying their evaluation model and the impacts on network system of deploying MTD techniques. In this method, the number of compromised nodes in cloud indicate the effectiveness of relevant technique. The

more nodes are protected, the more effective the defense/technique is. Furthermore, the advantage of this model is that it takes into consideration of both formal attack model and allows the testbed close to real as possible. Also, it generates quantification results that enables further enhancement.

In [38], Crouse et al. propose a probabilistic model to evaluate MTD techniques. This model is specified on defending network reconnaissance and have a deeper research on evaluating the performance on the honeypots for deception and networking address shuffling for MTD. In this model, attack success rate is quantified in different dimension such as network size, implementation size or the number of compromised hosts. Furthermore, this model indicates that a more effective deployment is an integrated deployment of several defense techniques. Also, they clarify the costs of reconnaissance attackers with their certain configuration. Combining the attack success rate and reconnaissance expense, a metric is generated to evaluate the effectiveness of defense. The advantage of this model is that it generated quantified results to demonstrate connections between attack configuration and cost, the effectiveness of single or layer deployment and proves, in a scale, the effectiveness of MTD techniques.

In [39], Zhuang et al. propose a simulation-based approach to assess the effectiveness of an MTD technique. First, they propose their design of resource mapping system (RSM), enforcing the security policy of each network applications and enhancing the configuration of network applications to add on loads of attackers. They then provide a simulation-based evaluation to study their design, which includes five parameters: attack interval, adaptation interval, number of nodes, adaptations per adaptation interval and attack success likelihood. In the evaluation, previous five parameters serve as metrics to indicate the effectiveness of defense. Based on the metrics, the evaluation is built on

Nessi2^[40], an existing network simulator. With this simulator as host, their simulation is based on AG, evaluation is given with judging five parameters of the simulator. The advantage of this evaluation method is that the effectiveness of MTD is clearly illustrated with quantified results.

In [41], Zaffranano et al. propose cyber quantification framework (CQF) perjurying a typical testbed for qualitatively evaluating network-based MTD techniques. Also, in [42], Eskridge et al. propose another testing method, namely virtual infrastructure for network emulation (VINE) and a case study implementing in App OS diversity. They provide developers with a series of tool which can be applied in assessing and evaluating MTD techniques.

Summary: Network-based MTD techniques have been researched most, there are model-based^[37-38], simulation-based^[39] and other evaluations^[36,41-42]. Previous studied evaluations are both quantitative methods. But on addressing the challenges on evaluating MTD techniques, HARM^[37] and evaluation in^[39] have not been verified in real-scenario and it merely concentrates on the evaluation of effectiveness while unable to evaluate the efficiency of the defense. Models proposed in^[38-39] consider both effectiveness and efficiency but lack of universality to be applied in the other techniques. Methods offered in [41] is quite different from others. They are integrated tools and, hopefully, are able to develop into generalized evaluating standard.

3.5 An overall evaluation

In [43], Eskridge et al. propose probabilistic learning attacker, dynamic defender (PLADD) based on FlipIt game. This evaluation method covers all different levels of MTD techniques. In this model, both defenders and attackers' behavior will be observed. Attacker's utility, defender's cost and an optimal deployment is given by certain equations. With the calculating the equation we can evaluate

the effectiveness of defense and figure out an efficiency configuration. In their works, they conduct calculations and simulations to verify the theoretical authentication. The advantage of the framework is there is quantified output explaining the value of MTD techniques and directions for further improvement. Besides, it considers both cost and effectiveness which may generate efficiency. However, there still lacks of real-world testing result is insufficient. Also, it is unable to assess the effectiveness of coevolution.

In [44] Connell W et al. Propose a framework for moving target defense quantification. This quantitative works to evaluate and compare two sets of MTD techniques without specifying which its category. The evaluation framework is based on a four-layer mathematical model. A specific equation stated in the article is used to compute the effectiveness of MTD. This result can not only be used in evaluating MTD techniques but also selecting a more optimal defense. As it is stated that it can accommodate any existing MTD as long as the knowledge blocks it affects is available. Also, the four-layer design is decoupling MTD application with its hardware, effectiveness can be calculated independently when new techniques are added into comparison.

Summary: In previous sections, we have studied evaluation methods by the category of MTD. But it is still complicated to simply combine different category-based evaluations into an overall evaluation due to the feature of MTD. Evaluations in [43-44] is generalized methods to evaluate different MTD techniques but some conditions will apply still. The relationship between overall evaluation and evaluations by category is more than adding or multiplying. The lack of a universalized security metrics is also the restrict of not foaming an effective overall evaluation. But an overall evaluation is often abstracted and inspired with the feature of techniques categorized to different layers.

Table 2 Quantitative metrics and evaluations on MTD

MTD category	Evaluation Approach	Metrics/Measurements
Data-based	Apache Server Experiment	Amount and content of error message
	Experiment on Data Randomization	The amount of unsafe accesses
	Experiment on DCR	The integrity of documents
	Nomad	Successful malicious posts
Software-based	Evaluation on Mvarmor	Probability to prevent advanced attacks
	Side Channel Security Experiment	Accuracy of AES side-channel
Runtime environment-based	Model of the Effectiveness of MTD	Probability of successful attacks
Platform-based	Quantitative Evaluation of DPT	Percentage of time that the attacker is in control
	GSPN	A self-define token
	Model on Parameterizing MTD	Probability of cyber-attack success rate
Network-based	A Cost-based Model	Tag space
	HARM	Attack success rate/saved nodes
	A Probabilistic Model on performance of MTD	Attack network size/compromised host
	A Simulation-based Approach	Time of complete attack and ratio of successful attack
	A Quantitative Framework	Productivity/ success and integrity of mission and attack

4 Open issues and discussions

After studying most of state-of-the-art evaluation methods and frameworks on MTD techniques, we can reach the following conclusions. 1) In most of evaluation methods, attack success rate, host-compromised rate or the probability of defense are considered the security metric. 2) The mainstream evaluation methods are simulation and experiment based, while a large portion of them is empirical deduction. Quantitative evaluation models or frameworks are mostly probabilistic and game theory based. 3) A majority of researches have been done in evaluating and assessing on dynamic runtime environment, dynamic platform and dynamic network techniques. Related work in dynamic data and dynamic software are lacking of generalized assessing models. 4) Most of existing quantitative evaluation approaches are capable of measuring both security effectiveness and deployment overheads. Yet, only a few of them combine them in one model to calculate the efficiency of defense implemented. 5) Some existing evaluation methods identify the most effective parts of technique being deployed and identify the effectiveness of a multi-layer-implementation.

With reviewing existing evaluation and security metrics on MTD techniques, throwing back to the

four challenges we have proposed at the beginning, there are issues remained to be discussed and solved.

1) Identification of impacts from other defense approaches. As in real world, we will implement diverse defense solutions in one computer or network system. Thus, it is essential to identify the impact (positive or negative in performance) on MTD techniques from the other defense approaches. However, existing evaluation seldom consider this issue because verifying experiment and evaluation models are often considered independently. 2) Still, there lack effective quantitative evaluation models. Empirical evaluations are necessary in abstracting defense effectiveness. Experiment-based evaluations may not be universalized enough for optimization in MTD. Thus model-based quantitative methods are indispensable in further improvement and configuration instruction. 3) The lack of generalized or universal evaluation methods. On describing attacks, CVSS and Lockheed Martin Cyber Kill Chain are often mention about. However, a generalized evaluation model or framework is yet to be surfaced. This is essential for comparing MTD techniques with different entities. 4) The formal security model adopted in evaluation approaches are another issue calls for open discussed. Many evaluations are not adopting security models but select specific vulnerabilities as testbed. This may result in limit evalua-

tion. 5) Apart from effectiveness, efficiency is also a significant factor to be considered. Few models consider defense effectiveness and cost as a whole and generate an interdependent evaluating result. When it comes to real scenario implementing, efficiency is worthy of noticing.

5 Conclusion

MTD techniques is of great potential in security defense. Therefore, quantitative evaluation methods are significant as they are essential for the improvement and development of MTD techniques. In this survey, a taxonomy of MTD techniques is introduced. Then a literature review of state-of-the-art quantitative evaluation methods and security metrics are proposed with comparison in accordance with different applying entities in computer system. The main merits and demerits of those methods and frameworks are described in details. Finally, a general conclusion and comparison is drawn, followed by issues to be solved and open discussions. Existing evaluation approaches are of great practical value. Besides, as advances have been achieved so far, this area proves to be in constant evolution and the development in the future is indeed promising.

References

- [1] JAJODIA S, GHOSH A K, SWARUP V, et al. Moving target defense[M]. Springer New York, 2011.
- [2] JAQUITH A. Security metrics: replacing fear, uncertainty, and doubt[M]. Addison-Wesley Professional, 2007.
- [3] OKHRAVI H, RABE M A, MAYBERRY T J, et al. Survey of cyber moving target techniques[R]. Massachusetts Inst of Tech Lexington Lincoln Lab, 2013.
- [4] OKHRAVI H, HOBSON T, BIGELOW D, et al. finding focus in the blur of moving-target techniques[J]. IEEE Security & Privacy, 2014, 12(2):16-26.
- [5] CADAR C, AKRITIDIS P, COSTA M, et al. Data randomization[R]. 2008.
- [6] CHANG W, STREIFF B, LIN C. Efficient and extensible security enforcement using dynamic data flow analysis[C]//ACM Conference on Computer and Communications Security. 2008: 39-50.
- [7] ALLEN R, DOUENCE R, GARLAN D. Specifying and analyzing dynamic software architectures[C]//International Conference on Fundamental Approaches To Software. DBLP, 1998:21-37.
- [8] HOORN A V, WALLER J, HASSELBRING W. Kieker: a framework for application performance monitoring and dynamic software analysis[C]//ACM/spec International Conference on PERFORMANCE Engineering. 2012:247-248.
- [9] ROEDER T, SCHNEIDER F B. Proactive obfuscation[J]. ACM Transactions on Computer Systems, 2009, 28(2):1973-1991.
- [10] BOYD S W, KC G S, LOCASIO M E, et al. On the general applicability of instruction-set randomization[J]. IEEE Transactions on Dependable and Secure Computing, 2010, 7(3): 255-270.
- [11] KIL C, JUN J, BOOKHOLT C, et al. Address space layout permutation (ASLP): towards fine-grained randomization of commodity software[C]//22nd Annual Computer Security Applications Conference, 2006 (ACSAC'06). 2006: 339-348.
- [12] FEDCHENKO O A. WO/2014/129928[P]. 2014.
- [13] ARONSON J E. A survey of dynamic network flows[J]. Annals of Operations Research, 1989, 20(1): 1-66.
- [14] CHANG H C, HSIEH M D, TSENG C C, et al. Dynamic network address translation system and method of transparent private network device: US, US7577144[P]. 2009.
- [15] ANTONATOS S S, AKRITIDIS P, MARKATOS E P, et al. Defending against hitlist worms using network address space randomization[J]. Computer Networks, 2007, 51(12):3471-3490.
- [16] ANDERSEN D G, BALAKRISHNAN H, KAASHOEK M F, et al. The case for resilient overlay networks[C]//The Workshop on Hot Topics in Operating Systems 2001, 35: 152-157.
- [17] MARTIN L. Cyber kill chain[EB/OL]. http://cyber.lockheedmartin.com/hubfs/Gaining_the_Advantage_Cyber_Kill_Chain.pdf, 2014.
- [18] OU X, SINGHAL A. The common vulnerability scoring system (CVSS)[M]//Quantitative Security Risk Assessment of Enterprise Networks. 2012:9-12.
- [19] MARCUS P, et al. A survey on systems security metrics[C]//ACM Computing Surveys (CSUR) 49.4. 2017: 62.
- [20] RAMOS A, LAZAR M, HOLANDA FILHO R, et al. Model-based quantitative network security metrics: a survey[J]. IEEE Communications Surveys & Tutorials, 2017, 19(4): 2704-2734.
- [21] WANG L, JAJODIA S, SINGHAL A. Network security metrics[M]. Berlin: Springer, 2017.
- [22] NGUYEN-TUONG A, EVANS D, KNIGHT J C, et al. Security through redundant data diversity[C]//Dependable Systems and Networks With FTCS and DCC, 2008. DSN 2008. IEEE International Conference on. IEEE, 2008: 187-196.
- [23] SMUTZ C, STAVROU A. Preventing exploits in microsoft office documents through content randomization[C]//International Workshop on Recent Advances in Intrusion Detection. 2015: 225-246.
- [24] VIKRAM S, YANG C, GU G. Nomad: Towards non-intrusive moving-target defense against web bots[C]//2013 IEEE Conference on Communications and Network Security (CNS). 2013: 55-63.
- [25] PATTUK E, KANTARCIOGLU M, LIN Z, et al. Preventing cryptographic key leakage in cloud virtual machines[C]//Usenix Conference on Security Symposium. 2014: 703-718.
- [26] AMMANN P E, KNIGHT J C. Data diversity: an approach to software fault tolerance[J]. IEEE Transactions on Computers, 1988, 37(4):418-425.
- [27] KONING K, BOS H, GIUFFRIDA C. Secure and efficient multi-variant execution using hardware-assisted process virtualization[C]//2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). 2016: 431-442.
- [28] CRANE S, HOMESCU A, BRUNTHALER S, et al. Thwarting cache side-channel attacks through dynamic software diversity[C]//NDSS. 2015: 8-11.
- [29] TROMER E, OSVIK D A, SHAMIR A. Efficient cache attacks on AES, and countermeasures[J]. Journal of Cryptology, 2010, 23(1): 37-71.

- [30] EVANS D, NGUYEN-TUONG A, KNIGHT J. Effectiveness of moving target defenses[M]//Moving Target Defense. Springer New York, 2011: 29-48.
- [31] OKHRAVI H, RIORDAN J, CARTER K. Quantitative evaluation of dynamic platform techniques as a defensive mechanism[C]//International Workshop on Recent Advances in Intrusion Detection. 2014: 405-425.
- [32] OKHRAVI H, COMELLA A, ROBINSON E, et al. Creating a cyber moving target for critical infrastructure applications using platform diversity[J]. International Journal of Critical Infrastructure Protection, 2012, 5(1): 30 -39.
- [33] CAI G, WANG B, LUO Y, et al. A model for evaluating and comparing moving target defense techniques based on generalized stochastic petri net[C]//Conference. Springer, Singapore, 2016: 184-197.
- [34] MARSAN M A, BALBO G, CONTE G, et al. Modelling with generalized stochastic petri nets[M]. John Wiley & Sons, Inc. 1995.
- [35] ANDERSON N, MITCHELL R, CHEN R. Parameterizing moving target defenses[C]//2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS). 2016: 1-6.
- [36] COLLINS M P. A cost-based mechanism for evaluating the effectiveness of moving target defenses[C]//International Conference on Decision and Game Theory for Security. 2012: 221-233.
- [37] HONG J B, KIM D S. Assessing the effectiveness of moving target defenses using security models[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(2): 163-177.
- [38] CROUSE M, PROSSER B, FULP E W. Probabilistic performance analysis of moving target and deception reconnaissance defenses[C]//The Second ACM Workshop on Moving Target Defense. 2015: 21-29.
- [39] ZHUANG R, ZHANG S, DELOACH S A, et al. Simulation-based approaches to studying effectiveness of moving-target network defense[C]//National Symposium on Moving Target Research. 2012: 1-12.
- [40] SCHMIDT S, BYE R, CHINNOW J, et al. Application-level simulation for network security[C]//International Conference on Simulation TOOLS and Techniques for Communications, Networks and Systems & Workshops. 2010:33.
- [41] ZAFFARANO K, TAYLOR J, HAMILTON S. A quantitative framework for moving target defense effectiveness evaluation[C]//The Second ACM Workshop on Moving Target Defense. 2015: 3-10.
- [42] ESKRIDGE T C, CARVALHO M M, STONER E, et al. VINE: a cyber emulation environment for MTD experimentation[C]//ACM Workshop on Moving Target Defense. 2015:43-47.
- [43] JONES S T, OUTKIN A V, GEARHART J L, et al. PLADD: deterring attacks on cyber systems and moving target defense[R]. 2017.
- [44] CONNELL W, ALBANESE M, VENKATESAN S. A framework for moving target defense quantification[M]// ICT Systems Security and Privacy Protection. 2017.

About the authors:



Huanruo LI, born in 1995, is pursuing a master degree at national digital switching system engineering technology research center. Her research interests include cyber security and active defense.



Yunfei GUO, born in 1963, is a PhD supervisor and a professor at national digital switching system engineering technology research center. His main research interests include cloud security, telecommunication network security and cyber security.



Shumin HUO, born in 1985, PhD, is a lecturer in national digital switching system engineering technology research center. His main research interests include cloud computing, software-defined network and cyber security.



Guozhen CHENG, born in 1986, PhD, is a lecturer in national digital switching system engineering technology research center. His main research interests include cloud computing, software-defined network and cyber security.



Wenyan LIU, born in 1986, PhD, is a lecturer in national digital switching system engineering technology research center. His main research interests include cloud computing, software-defined network and cyber security.