2.6 攻击面动态转移的策略

目前的攻击面动态转移方法大多都依赖于针对某些特定攻击,对相应的攻击面进行转移,从而实现抵御攻击、维护系统安全的目的.然而,对于如何进行转移、何时进行转移的问题,很多研究者在实行攻击面的动态转移时并没有充分考虑.于是,攻击面动态转移的策略的研究便应运而生.

关于博弈论方法的研究由来已久,而很大一部分研究者便将其融入到攻击面动态转移的策略研究中.通过对攻击者和防御方之间的动作、状态、攻击面转移作为特征,以双方的收益与付出作为评估标准,将攻击方和防御方之间的攻防过程建立博弈模型,以此求解防御方的最佳攻击面转移策略.Manadhata[97]从二人博弈的角度出发,对防御者和攻击者之间的相互关系进行建模,构造双方的回报函数,运用博弈论的方法来确定最佳的防御策略.但是该博弈方法是一种完全且完美的信息博弈,双方都清楚知晓对方的策略和回报,并且熟悉博弈之间已采取的各项操作,这种博弈方式不符合实际情况.Carter 等人[98]为了使得博弈过程更符合实际情况,假定攻击者拥有全部信息而防御者只拥有部分信息,构建攻防双方不完全信息的博弈,同时,对于静态攻击者和根据防御行为自适应改变攻击行为的这两类攻击者,分别建立模型,以此制定相应的防御决策.Wright 等人[99]针对前期研究中抵御 DDoS 攻击的一些防御手段,通过仿真的方式对其进行博弈论分析,以此评估攻击面转移策略在不同环境下的有效性和合理性.Feng 等人[100]向攻击面的动态转移策略方法中引入了信号传递博弈,通过防御者在执行转移行为后向攻击者泄露部分已部署的防御策略的方式,对攻击者后续的攻击行为造成干扰和影响,构建双方的贝叶斯斯塔克尔伯格博弈模型,以此寻求最佳的攻击面动态转移策略.

基于 Markov 模型的策略生成方法,也受到了一部分研究者的关注.Miehling 等人[101]对攻击者的可利用漏洞、攻击成功率、攻击路径等进行建模,并假设防御者只在特定时间才能观测到攻击行为并采取一定防御措施,同时对防御行为的开销进行定义,并将部分可观测马尔可夫决策过程模型(POMDP)引入其中,以此计算出可供选择的几种策略方案.Maleki 等人[102]将大量的攻击面转移技术抽象化,并为攻击面的动态转移过程建立 Markov 模型,以此评估攻击者攻击成功的概率与攻击者耗费时间与开销之间的关系;同时,根据该模型定义了安全强度的概念,以此来测量不同攻击面动态转移策略的有效性.Lei 等人[103]针对网络层攻击面的动态转移技术构建攻防双方的 Markov 博弈模型,其中兼顾双方、状态、攻防策略、转移概率、收益等.通过 Markov 决策过程描述网络状态在攻防进行博弈情况下的转移过程,并计算攻防双方的收益矩阵,以此选择最佳的防御策略.

此外,雷程和马多贺等人[73,74]提出的基于网络攻击面的自适应转换技术,通过对网络中攻击者扫描策略的感知和分析,制定出对应的转移策略,进行网络攻击面上端信息的跳变,也为后续攻击面动态转移策略的研究提供了一些思路.

3 未来研究方向展望

3.1 多层次攻击面动态转移技术的融合

尽管目前的攻击面动态转移方法能够通过改变特定系统资源属性或属性对外的呈现信息,使其攻击面发生变化,从而迷惑或误导攻击者,促使攻击者攻击错误目标或丢失攻击目标,改变网络防御的被动态势,提高系统的安全性,但是目前的攻击面转移技术大多只针对特定的某一类攻击或者某一攻击面而展开研究,这也导致目前的动态防御方法的适用范围较小.在不干扰现有安全防御手段的前提下,如何实现多层次攻击面动态转移技术的融合,形成体系化、系统化的动态防御体系,达到整体联动的动态防御效果,将需要进一步的研究.

3.2 攻击面动态转移的综合评估方法

进行攻击面的动态转移能否减小系统攻击面、提高系统安全等级、是否会对系统的可用性和性能造成影响,都是防御者最为关注的几个方面.目前的攻击面动态转移的评估方法中,大多集中在于攻击面的动态转移对于防御的有效性.同时,也有部分研究者提出基于 I/O 自动机的攻击面模型[8]、Markov 转移概率模型[97]、攻击图(attack graph)转移模型[104],通过这些模型,形式化地刻画攻击面的转移,并定量地对攻击面的转移以及防御的有效性、转移开销、性能耗费进行评估.但是,目前现有的这些评估手段大都由研究者针对特定攻击面的转移

提出,尚不成熟.而且目前的评估方法大多针对有效性,缺乏转移开销、性能耗费的评估,也缺少与不同类别转移技术的对比评估.因此,结合第 3.1 节中所提及的多层次攻击面转移的动态防御体系,实现定量描述系统攻击面的转移变化,综合评估系统的安全状态以及动态防御体系的有效性和开销,与不同类型转换技术的比较评估,将会是未来研究的一大方向.

3.3 基于威胁感知的攻击面动态转移方法

目前的攻击面动态转移方法大多缺乏对攻击以及威胁的动态感知,导致动态转移决策的选取具有盲目性.然而,盲目随机的转移方法一方面将极大地降低防御的有效性,另一方面,也会给系统带来较大的性能开销.虽然已经有部分研究者在网络攻击面上针对网络扫描阶段进行网络威胁的感知,分析攻击者的不同扫描策略行为,以指导后续的转移策略的生成[73,74],但是目前的研究仅处于起步阶段,具有一定的局限性.因此,如何实现系统的威胁感知,进行威胁信息的关联、融合,同时针对感知到的系统当前面临的威胁信息,有针对性地对相关的攻击面进行动态转移,以此制定出攻击面动态转移的最优转移策略,提升攻击面动态转移技术的有效性,将成为后续的一大研究方向.

3.4 基于三方博弈模型的攻击面转移决策

由于在攻击面动态转移的过程中,防御者为了减小系统的攻击面,往往需要修改或者禁用系统的某些特征;而系统在进行某项作业时,可能需要启用某些新特征或者修改某些原有特征,也存在着增大系统攻击面的可能.于是,防御者在实施动态转移攻击面的同时,必须在系统的安全性和可用性之间进行权衡,关于攻击面动态转移的决策方法的研究也随之应运而生.目前,主流的决策手段主要基于博弈论方法[105,106],通过对攻防双方的攻击行为、防御行为以及系统状态、行动回报等建立博弈模型,求解出使得防御方回报最大化的策略,据此来实行攻击面动态转移的决策.但是,目前基于博弈论的决策方法仅仅建立在攻击方和防御方两方上,并没有考虑到用户方参与博弈的情况.而且,该方法建立在攻防两方互相知晓对方的策略和回报的基础上,博弈模型还不够完善.于是,考虑到用户方的参与,如何建立预测博弈的后续行动和状态的三方博弈模型,兼顾安全成本和安全收益,可能将成为后续攻击面转移决策的一个研究方向.

4 结束语

攻击面的动态转移技术一直以来都是移动目标防御领域的重点问题.随着网络攻击技术和防御技术的不断演化与发展,该研究一直受到研究人员的广泛关注.针对这一问题,本文首先梳理了攻击面以及其动态转移的基本概念,然后从数据攻击面、软件攻击面、网络攻击面和平台攻击面这 4 个层次分别介绍了攻击面的动态转移技术,并对不同的转移技术进行分析和比较,分别指出它们的优点和缺陷,也得到了一些初步的结论.

我们认为,对攻击面动态转移技术研究的理解应体现在以下 5 个方面.

1) 攻击目标可变.当前,网络系统的确定性、静态性和同构性使得攻击者具有时间优势、信息不对称优势以及成本优势,也导致防御者自始至终处在被动的劣势地位.需要确定可变化的攻击面资源,通过动态转移,使得攻击面呈现出多样的变化,从而使得攻击面面对变化的攻击目标而无法实施针对性的攻击;
2) 资源实时掌握.知己知彼,百战不殆.防御者在作出攻击面动态转移的相关决策时,首先需要的便是对攻击面上存在资源的实时状态有着充分的了解,在面对攻击时,根据系统各层攻击面的实时情况,才能作出正确的防御决策,保证攻击面动态转移的有效性;
3) 响应转移迅速.在面对来势汹汹的进攻时,一方面需要保证攻击面动态转移的有效性,另一方面,防御方需要迅速作出响应,在攻击者进一步渗透系统其他资源之前,实现攻击面的动态转移,保证转移的时效性;
4) 攻击面转移可持续.在面对攻击者的攻击进行攻击面的动态转移时,不仅需要考虑规避攻击、提升系统安全,还要考虑动态转移的防御成本以及维护系统持续正常运行的性能,实现攻击面动态转移的

“可持续发展”;

5) 全方位攻击面转移.随着攻击手段的不断发展壮大,许多单一层次的攻击面转移往往存在着这样的问题:在进行某一攻击面动态转移的同时,反而暴露给攻击者其他层面的可利用的资源,仍然存在可乘之机.因此,要达到更好的防御效果,就需要多层次、全方位的攻击面动态转移,促使攻击者难以获取可利用资源,降低其攻击成功率.

目前,国内外有关攻击面动态转移技术的研究正处于快速发展的阶段,虽然已经有大量的具体实现的攻击面动态转移手段被提出,但其中也存在一些重要的研究方向才初步涉及,研究还没有深入开展,例如制定攻击面动态转移策略的相关研究、自适应的攻击面动态转移研究等.此外,还有许多其他的研究方面尚未涉及到,例如多层次融合的攻击面动态转移技术研究、攻击面动态转移的综合效能评估方法研究、基于威胁感知的攻击面动态转移方法研究、基于三方博弈的新型攻击面转移策略研究等,这些也在文中未来展望中有所提及,希望能够为后续的相关研究工作的开展提供建议与参考.

References:

[1] Jajodia S, Ghosh AK, Swarup V, *et al*. Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats. New York: Springer Science & Business Media, 2011. 1–5.

[2] Zhang XY, Li ZH. Overview on moving target defense technology. Communications Technology, 2013,46(6):111−113 (in Chinese with English abstract).

[3] Cai GL, Wang BS, Wang TZ, *et al*. Research and development of moving target defense technology. Journal of Computer Research and Development, 2016,53(5):968−987 (in Chinese with English abstract).

[4] Jajodia S, Ghosh AK, Subrahmanian VS, *et al*. Moving Target Defense II: Application of Game Theory and Adversarial Modeling. New York: Springer Science & Business Media, 2013. 15−40.

[5] Okhravi H, Rabe MA, Mayberry TJ, *et al*. Survey of cyber moving target techniques. TR-1166. Lexington: Massachusetts Inst of Tech Lexington Lincoln Lab, 2013. 1–149.

[6] Howard M, Pincus J, Wing JM. Measuring relative attack surfaces. In: Lee DT, Shieh SP, Tygar JD, eds. Computer Security in the 21st Century. 2003. 109−137.

[7] Manadhata PK, Tan KM, Maxion RA, *et al*. An approach to measuring a system’s attack surface. No.0704-0188. Pittsburgh: Carnegie-Mellon Univ Pittsburgh Pa School of Computer Science, 2007. 1–29.

[8] Manadhata PK, Wing JM. An attack surface metric. IEEE Trans. on Software Engineering, 2011,37(3):371−386.

[9] Kurmus A, Tartler R, Dorneanu D, *et al*. Attack surface metrics and automated compile-time OS kernel tailoring. In: Proc. of the 20th Annual Network & Distributed System Security Symp. (NDSS). San Diego, 2013.

[10] Peng W, Li F, Huang CT, *et al*. A moving-target defense strategy for cloud-based services with heterogeneous and dynamic attack surfaces. In: Proc. of the 2014 IEEE Int’l Conf. on Communications (ICC). IEEE, 2014. 804–809.

[11] Foreman JC, Gurugubelli D. Identifying the cyber attack surface of the advanced metering infrastructure. The Electricity Journal, 2015,28(1):94−103.

[12] Sun K, Jajodia S. Protecting enterprise networks through attack surface expansion. In: Proc. of the 2014 Workshop on Cyber Security Analytics, Intelligence and Automation. ACM Press, 2014. 29–32.

[13] Cybenko G, Jajodia S, Wellman MP, *et al*. Adversarial and uncertain reasoning for adaptive cyber defense: Building the scientific foundation. In: Proc. of the Int’l Conf. on Information Systems Security. Cham: Springer-Verlag, 2014. 1–8.

[14] Bopche GS, Mehtre BM. Graph similarity metrics for assessing temporal changes in attack surface of dynamic networks. Computers & Security, 2017,64:16−43.

[15] Cadar C, Akritidis P, Costa M, *et al*. Data randomization. Technical Report, TR-2008-120, Cambridge: Microsoft Research, 2008.

[16] Man YJ, Yin Q, Zhu XD. Fine-Grained data randomization technique based on field-sensitive pointer analysis. Journal of Computer Applications, 2016,36(6):1567−1572 (in Chinese English abstract).

[17] Fen Y, Fuchao Y, Xiaobing S, *et al*. A new data randomization method to defend buffer overflow attacks. Physics Procedia, 2012, 24:1757−1764.

[18] Gentry C. Fully homomorphic encryption using ideal lattices. In: Proc. of the 41st Annual ACM Symp. on Theory of Computing (STOC). 2009,9(4):169−178.

[19] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping. ACM Trans. on Computation Theory (TOCT), 2014,6(3):13.

[20] Brakerski Z. Fully homomorphic encryption without modulus switching from classical GapSVP. In: Safavi-Naini R, Canetti R, eds. Proc. of the Advances in Cryptology (CRYPTO 2012). LNCS, Berlin: Springer-Verlag, 2012. 868−886.

[21] Berkoff A, Liu FH. Leakage resilient fully homomorphic encryption. In: Proc. of the Theory of Cryptography Conf. Berlin, Heidelberg: Springer-Verlag, 2014. 515−539.

[22] Ducas L, Micciancio D. FHEW: Bootstrapping homomorphic encryption in less than a second. In: Proc. of the Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer-Verlag, 2015. 617−640.

[23] Lai J, Deng RH, Ma C, *et al*. CCA-Secure keyed-fully homomorphic encryption. In: Cheng CM, Chung KM, Persiano G, Yang BY, eds. Proc. of the Public-Key Cryptography (PKC 2016). LNCS, Berlin: Springer-Verlag, 2016. 70−98.

[24] Ammann PE, Knight JC. Data diversity: An approach to software fault tolerance. IEEE Trans. on Computers, 1988,37(4):418−425.

[25] Nguyen-Tuong A, Evans D, Knight JC, *et al*. Security through redundant data diversity. In: Proc. of the IEEE Int'l Conf. on Dependable Systems and Networks with FTCS and DCC (DSN 2008). IEEE, 2008. 187−196.

[26] Barus AC, Chen TY, Kuo FC, *et al*. A cost-effective random testing method for programs with non-numeric inputs. IEEE Trans. on Computers, 2016,65(12):3509−3523.

[27] Liu H, Chen TY. Randomized quasi-random testing. IEEE Trans. on Computers, 2016,65(6):1896−1909.

[28] Mitropoulos D, Spinellis D. Fatal injection: A survey of modern code injection attack countermeasures. PeerJ Computer Science, 2017,3:e136.

[29] Nashimoto S, Homma N, Hayashi Y, *et al*. Buffer overflow attack with multiple fault injection and a proven countermeasure. Journal of Cryptographic Engineering, 2017,7(1):35−46.

[30] Prandini M, Ramilli M. Return-Oriented programming. IEEE Security & Privacy, 2012,10(6):84−87.

[31] Alneyadi S, Sithirasenan E, Muthukkumarasamy V. A survey on data leakage prevention systems. Journal of Network and Computer Applications, 2016,62:137−152.

[32] Lin J, Mi C, Shi Y. Approach of tamper detection for sensitive data based on negotiable hash algorithm. Int'l Journal of Performability Engineering, 2017,13(5):711.

[33] Forrest S, Somayaji A, Ackley DH. Building diverse computer systems. In: Proc. of the 6th Workshop on Hot Topics in Operating Systems. IEEE, 1997. 67−72.

[34] Seo J, Lee B, Kim S, *et al*. SGX-Shield: Enabling address space layout randomization for SGX programs. In: Proc. of the 2017 Annual Network and Distributed System Security Symp. (NDSS). San Diego, 2017.

[35] Chen Y, Wang Z, Whalley D, *et al*. Remix: On-demand live randomization. In: Proc. of the 6th ACM Conf. on Data and Application Security and Privacy. ACM Press, 2016. 50−61.

[36] Werner J, Baltas G, Dallara R, *et al*. No-Execute-After-Read: Preventing code disclosure in commodity software. In: Proc. of the 11th ACM on Asia Conf. on Computer and Communications Security. ACM Press, 2016. 35−46.

[37] Gras B, Razavi K, Bosman E, *et al*. ASLR on the line: Practical cache attacks on the MMU. In: Proc. of the 2017 Annual Network and Distributed System Security Symp. (NDSS). San Diego, 2017.

[38] Thimbleby H. Can viruses ever be useful? Computers & Security, 1991,10(2):111−114.

[39] Geneiatakis D. Minimizing databases attack surface against SQL injection attacks. In: Proc. of the Int'l Conf. on Information and Communications Security. Springer Int'l Publishing, 2015. 1−9.

[40] Ping C, Jinshuang W, Lin P, *et al*. Research and implementation of SQL injection prevention method based on ISR. In: Proc. of the 2016 2nd IEEE Int'l Conf. on Computer and Communications (ICCC). IEEE, 2016. 1153−1156.

[41] Wartell R, Mohan V, Hamlen KW, *et al*. Binary stirring: Self-randomizing instruction addresses of legacy x86 binary code. In: Proc. of the 2012 ACM Conf. on Computer and Communications Security. ACM Press, 2012. 157−168.

[42] Venkat A, Shamasunder S, Shacham H, *et al*. Hipstr: Heterogeneous-isa program state relocation. ACM SIGARCH Computer Architecture News, 2016,44(2):727−741.

[43] Sinha K, Kemerlis VP, Sethumadhavan S. Reviving instruction set randomization. In: Proc. of the 2017 IEEE Int'l Symp. on Hardware Oriented Security and Trust (HOST). IEEE, 2017. 21−28.

[44] Lee J, Jang J, Jang Y, *et al*. Hacking in darkness: Return-oriented programming against secure enclaves. In: Proc. of the USENIX Security. 2017. 523−539.

[45] Tran M, Etheridge M, Bletsch T, *et al*. On the expressiveness of return-into-libc attacks. In: Proc. of the Recent Advances in Intrusion Detection. Berlin, Heidelberg: Springer-Verlag, 2011. 121−141.

[46] Ruan Y, Kalyanasundaram S, Zou X. Survey of return-oriented programming defense mechanisms. Security and Communication Networks, 2016,9(10):1247−1265.

[47] Pappas V, Polychronakis M, Keromytis AD. Smashing the gadgets: Hindering return-oriented programming using in-place code randomization. In: Proc. of the 2012 IEEE Symp. on Security and Privacy (SP). IEEE, 2012. 601−615.

[48] Koo H, Polychronakis M. Juggling the gadgets: Binary-level code randomization using instruction displacement. In: Proc. of the 11th ACM on Asia Conf. on Computer and Communications Security. ACM Press, 2016. 23−34.

[49] Chen X, Bos H, Giuffrida C. CodeArmor: Virtualizing the code space to counter disclosure attacks. In: Proc. of the 2017 IEEE European Symp. on Security and Privacy (EuroS&P). IEEE, 2017. 514−529.

[50] Snow KZ, Monrose F, Davi L, *et al*. Just-in-Time code reuse: On the effectiveness of fine-grained address space layout randomization. In: Proc. of the 2013 IEEE Symp. on Security and Privacy (SP). IEEE, 2013. 574−588.

[51] Carlini N, Wagner D. ROP is still dangerous: Breaking modern defenses. In: Proc. of the USENIX Security Symp. 2014. 385−399.

[52] Maisuradze G, Backes M, Rossow C. What cannot be read, cannot be leveraged? Revisiting assumptions of JIT-ROP defenses. In: Proc. of the USENIX Security Symp. 2016. 139−156.

[53] Temizkan O, Park S, Saydam C. Software diversity for improved network security: Optimal distribution of software-based shared vulnerabilities. Information Systems Research, 2017,28(4):828−849.

[54] Cui W, Peinado M, Cha SK, *et al*. Retracer: Triaging crashes by reverse execution from partial memory dumps. In: Proc. of the 38th Int'l Conf. on Software Engineering. ACM Press, 2016. 820−831.

[55] Crane S, Liebchen C, Homescu A, *et al*. Readactor: Practical code randomization resilient to memory disclosure. In: Proc. of the 2015 IEEE Symp. on Security and Privacy (SP). IEEE, 2015. 763−780.

[56] Tagatac DM, Polychronakis M, Stolfo SJ. Using diversity to harden multithreaded programs against exploitation. 2016 IEEE 2nd Int'l Conf. on Big Data Security on Cloud (BigDataSecurity), IEEE Int'l Conf. on High Performance and Smart Computing (HPSC), and IEEE Int'l Conf. on Intelligent Data and Security (IDS). IEEE, 2016. 208−213.

[57] Shterenberg SI, Krasov AV, Ushakov IA. Analysis of using equivalent instructions at the hidden embedding of information into the executable files. Journal of Theoretical and Applied Information Technology, 2015,80(1):28.

[58] Volckaert S, Coppens B, De Sutter B. Cloning your gadgets: Complete ROP attack immunity with multi-variant execution. IEEE Trans. on Dependable and Secure Computing, 2016,13(4):437−450.

[59] Volckaert S, Coppens B, De Sutter B, *et al*. Taming parallelism in a multi-variant execution environment. In: Proc. of the 12th European Conf. on Computer Systems. ACM Press, 2017. 270−285.

[60] Al-Shaer E. Toward network configuration randomization for moving target defense. In: Jajodia S, Ghosh AK, Swarup V, *et al*, eds. Proc. of the Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats. New York: Springer Science & Business Media, 2011. 153−159.

[61] Yackoski J, Bullen H, Yu X, *et al*. Applying self-shielding dynamics to the network architecture. In: Jajodia S, Ghosh AK, Swarup V, *et al*, eds. Proc. of the Moving Target Defense II: Application of Game Theory and Adversarial Modeling. New York: Springer Science & Business Media, 2013. 97−115.

[62] Yackoski J, Li J, DeLoach SA, *et al*. Mission-Oriented moving target defense based on cryptographically strong network dynamics. In: Proc. of the 8th Annual Cyber Security and Information Intelligence Research Workshop. ACM Press, 2013. 57.

[63] Jia Q, Sun K, Stavrou A. Motag: Moving target defense against internet denial of service attacks. In: Proc. of the 2013 22nd Int'l Conf. on Computer Communications and Networks (ICCCN). IEEE, 2013. 1−9.

[64] Albanese M, De Benedictis A, Jajodia S, *et al*. A moving target defense mechanism for Manets based on identity virtualization. In: Proc. of the 2013 IEEE Conf. on Communications and Network Security (CNS). IEEE, 2013. 278−286.

[65] Kampanakis P, Perros H, Beyene T. SDN-Based solutions for moving target defense network protection. In: Proc. of the 2014 IEEE 15th Int'l Symp. on a World of Wireless, Mobile and Multimedia Networks (WoWMoM). IEEE, 2014. 1−6.

[66] Wang L, Wu D. Moving target defense against network reconnaissance with software defined networking. In: Proc. of the Int'l Conf. on Information Security. Cham: Springer-Verlag, 2016. 203−217.

[67] Jafarian JH, Al-Shaer E, Duan Q. Openflow random host mutation: Transparent moving target defense using software defined networking. In: Proc. of the 1st Workshop on Hot Topics in Software Defined Networks. ACM Press, 2012. 127−132.

[68] Jafarian JHH, Al-Shaer E, Duan Q. Spatio-Temporal address mutation for proactive cyber agility against sophisticated attackers. In: Proc. of the 1st ACM Workshop on Moving Target Defense. ACM Press, 2014. 69−78.

[69] Wang S, Zhang L, Tang C. A new dynamic address solution for moving target defense. In: Proc. of the Information Technology, Networking, Electronic and Automation Control Conf., IEEE. IEEE, 2016. 1149−1152.

[70] Makanju A, Zincir-Heywood AN, Kiyomoto S. On evolutionary computation for moving target defense in software defined networks. In: Proc. of the Genetic and Evolutionary Computation Conf. on Companion. ACM Press, 2017. 287−288.

[71] Lin K, Jia CF. End hopping based on message tampering. Journal on Communications, 2013,34(12):142−148 (in Chinese with English abstract)

[72] Luo YB, Wang BS, Wang XF, *et al*. RPAH: Random port and address hopping for thwarting internal and external adversaries. In: Proc. of the 2015 IEEE Trustcom/BigDataSE/ISPA. IEEE, 2015. 263−270.

[73] Ma D, Lei C, Wang L, *et al*. A self-adaptive hopping approach of moving target defense to thwart scanning attacks. In: Proc. of the Int'l Conf. on Information and Communications Security. Cham: Springer-Verlag, 2016. 39−53.

[74] Lei C, Ma DH, Zhang HQ, Yang YJ, Wang LM. Moving target defense technique based on network attack surface self-adaptive mutation. Chinese Journal of Computers, 2018,41(5):1109−1131 (in Chinese with English abstract). http://kns.cnki.net/kcms/detail/11.1826.TP.20170819.0034.010.html

[75] Zhao Z, Gong D, Lu B, *et al*. SDN-Based double hopping communication against sniffer attack. In: Proc. of the Mathematical Problems in Engineering, 2016. 2016.

[76] Lucas B, Fulp EW, John DJ, *et al*. An initial framework for evolving computer configurations as a moving target defense. In: Proc. of the 9th Annual Cyber and Information Security Research Conf. ACM Press, 2014. 69−72.

[77] John DJ, Smith RW, Turkett WH, *et al*. Evolutionary based moving target cyber defense. In: Proc. of the Companion Publication of the 2014 Annual Conf. on Genetic and Evolutionary Computation. ACM Press, 2014. 1261−1268.

[78] Thompson M, Evans N, Kisekka V. Multiple OS rotational environment an implemented moving target defense. In: Proc. of the 2014 7th Int'l Symp. on Resilient Control Systems (ISRCS). IEEE, 2014. 1−6.

[79] Thompson M, Mendolla M, Muggler M, *et al*. Dynamic application rotation environment for moving target defense. In: Proc. of the 2016 Resilience Week (RWS). IEEE, 2016. 17−26.

[80] Debroy S, Calyam P, Nguyen M, *et al*. Frequency-Minimal moving target defense using software-defined networking. In: Proc. of the 2016 Int'l Conf. on Computing, Networking and Communications (ICNC). IEEE, 2016. 1−6.

[81] Okhravi H, Comella A, Robinson E, *et al*. Creating a cyber moving target for critical infrastructure applications using platform diversity. Int'l Journal of Critical Infrastructure Protection, 2012,5(1):30−39.

[82] Bangalore AK, Sood AK. Securing Web servers using self cleansing intrusion tolerance (scit). In: Proc. of the 2nd Int'l Conf. on Dependability 2009 (DEPEND 2009). IEEE, 2009. 60−65.

[83] Huang Y, Ghosh AK. Introducing diversity and uncertainty to create moving attack surfaces for web services. In: Jajodia S, Ghosh AK, Swarup V, *et al*, eds. Proc. of the Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats. New York: Springer Science & Business Media, 2011. 131−151.

[84] Nguyen QL, Sood A. Scalability of cloud based SCIT-MTD. In: Proc. of the 2017 IEEE Int'l Conf. on Software Quality, Reliability and Security Companion (QRS-C). IEEE, 2017. 581−582.

[85] Jia Q, Wang H, Fleck D, *et al*. Catch me if you can: A cloud-enabled ddos defense. In: Proc. of the 2014 44th Annual IEEE/IFIP Int'l Conf. on Dependable Systems and Networks (DSN). IEEE, 2014. 264−275.

[86] Al-Salah T, Hong L, Shetty S. Attack surface expansion using decoys to protect virtualized infrastructure. In: Proc. of the 2017 IEEE Int'l Conf. on Edge Computing (EDGE). IEEE, 2017. 216−219.

[87] Huang R, Zhang H, Liu Y, *et al*. RELOCATE: A container based moving target defense approach. In: Proc. of the 2017 7th Int'l Conf. on Computer Engineering and Networks (CENet 2017). Shanghai, 2017. href="https://pos.sissa.it/cgi-bin/reader/conf.cgi?confid=299">https://pos.sissa.it/cgi-bin/reader/conf.cgi?confid=299,id.8

[88] Vadlamudi SG, Sengupta S, Taguinod M, *et al*. Moving target defense for Web applications using bayesian stackelberg games. In: Proc. of the 2016 Int'l Conf. on Autonomous Agents & Multiagent Systems. Int'l Foundation for Autonomous Agents and Multiagent Systems, 2016. 1377−1378.

[89] Sengupta S, Vadlamudi SG, Kambhampati S, *et al*. A game theoretic approach to strategy generation for moving target defense in Web applications. In: Proc. of the 16th Conf. on Autonomous Agents and MultiAgent Systems. Int'l Foundation for Autonomous Agents and Multiagent Systems, 2017. 178−186.

[90] Heydari V, Kim S, Yoo SM. Anti-Censorship framework using mobile ipv6 based moving target defense. In: Proc. of the 11th Annual Cyber and Information Security Research Conf. ACM Press, 2016. 7.

[91] Heydari V, Kim S, Yoo SM. Scalable anti-censorship framework using moving target defense for Web servers. IEEE Trans. on Information Forensics and Security, 2017,12(5):1113−1124.

[92] Niakanlahiji A, Jafarian JH. WebMTD: Defeating Web code injection attacks using Web element attribute mutation. In: Proc. of the 2017 Workshop on Moving Target Defense. ACM Press, 2017. 17−26.

[93] Lee B, Lu L, Wang T, *et al*. From zygote to morula: Fortifying weakened aslr on android. In: Proc. of the 2014 IEEE Symp. on Security and Privacy (SP). IEEE, 2014. 424−439.

[94] Liang Y, Ma X, Wu D, *et al*. Stack layout randomization with minimal rewriting of Android binaries. In: Proc. of the Int'l Conf. on Information Security and Cryptology. Springer Int'l Publishing, 2015. 229−245.

[95] Braden K, Davi L, Liebchen C, *et al*. Leakage-Resilient layout randomization for mobile devices. In: Proc. of the 20th Annual Network & Distributed System Security Symp. (NDSS). San Diego, 2016.

[96] Parikh V, Mateti P. ASLR and ROP attack mitigations for ARM-based android devices. In: Proc. of the Int'l Symp. on Security in Computing and Communication. Singapore: Springer-Verlag, 2017. 350−363.

[97] Manadhata PK. Game theoretic approaches to attack surface shifting. In: Jajodia S, Ghosh AK, Swarup V, *et al*, eds. Proc. of the Moving Target Defense II: Application of Game Theory and Adversarial Modeling. New York: Springer Science & Business Media, 2013. 1−13.

[98] Carter KM, Riordan JF, Okhravi H. A game theoretic approach to strategy determination for dynamic platform defenses. In: Proc. of the 1st ACM Workshop on Moving Target Defense. ACM Press, 2014. 21−30.

[99] Wright M, Venkatesan S, Albanese M, *et al*. Moving target defense against DDoS attacks: An empirical game-theoretic analysis. In: Proc. of the 3rd ACM Workshop on Moving Target Defense. ACM Press, 2016. 93−104.

[100] Feng X, Zheng Z, Cansever D, *et al*. A signaling game model for moving target defense. In: Proc. of the INFOCOM 2017—IEEE Conf. on Computer Communications. IEEE, 2017. 1−9.

[101] Miehling E, Rasouli M, Teneketzis D. Optimal defense policies for partially observable spreading processes on bayesian attack graphs. In: Proc. of the 2nd ACM Workshop on Moving Target Defense. ACM Press, 2015. 67−76.

[102] Maleki H, Valizadeh S, Koch W, *et al*. Markov modeling of moving target defense games. In: Proc. of the 3rd ACM Workshop on Moving Target Defense. ACM Press, 2016. 81−92.

[103] Lei C, Ma DH, Zhang HQ. Optimal strategy selection for moving target defense based on Markov game. IEEE Access, 2017,5: 156−169.

[104] Zhuang R, DeLoach SA, Ou X. A model for analyzing the effect of moving target defenses on enterprise networks. In: Proc. of the 9th Annual Cyber and Information Security Research Conf. ACM Press, 2014. 73−76.

[105] Do CT, Tran NH, Hong C, *et al*. Game theory for cyber security and privacy. ACM Computing Surveys (CSUR), 2017,50(2):30.

[106] Nguyen TH, Wright M, Wellman MP, *et al*. Multi-Stage attack graph security games: Heuristic strategies, with empirical game-theoretic analysis. In: Proc. of the 2017 Workshop on Moving Target Defense. ACM Press, 2017. 17−26.

附中文参考文献:

[2] 张晓玉,李振邦.移动目标防御技术综述.通信技术,2013,46(6):111−113.

[3] 蔡桂林,王宝生,王天佐,等.移动目标防御技术研究进展.计算机研究与发展,2016,53(5):968−987.

[16] 蔺羽佳,尹青,朱晓东.基于域敏感指针分析的细粒度数据随机化技术.计算机应用,2016,36(6):1567−1572.

[71] 林楷,贾春福.基于消息篡改的端信息跳变技术.通信学报,2013,(12):142−148.

[74] 雷程,马多贺,张红旗,杨英杰,王利明.基于网络攻击面自适应转换的移动目标防御技术.计算机学报,2018,41(5):1109−1131. http://kns.cnki. net/kcms/detail/11.1826.TP.20170819.0034.010.html

周余阳(1994－),男,江苏泰州人,博士生,主要研究领域为网络安全,移动目标防御.

郭春生(1994－),男,硕士生,主要研究领域为网络安全.

程光(1973－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为网络空间安全监测和防护,网络大数据分析.

戴冕(1988－),男,博士生,主要研究领域为软件定义网络,数据中心网络,网络测量技术.