DOI:10.3969/j.issn.1009-6868.2016.01.009
网络出版地址:http://www.cnki.net/kcms/detail/34.1228.TN.20151216.2117.002.html

动态网络主动安全防御的若干思考

Proactive Security Defense of Dynamic Network

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2016) 01-0034-004

摘要: 提出以动态化、随机化、主动化为特点的动态网络主动安全防御是解决信息系统中未知漏洞与后门攻击的一种新途径。在动态网络的主动变迁技术中,提出了演进防御机制(EDM),该机制可以根据网络系统安全状态、网络系统安全需求等,选择最佳的网络配置变化元素组合来应对潜在的攻击、保证特定等级的安全要求。网络的动态重构和变迁需要根据系统的安全态势和可能遭受的网络攻击来考虑,其关键是如何有效对系统的安全态势和网络的攻击进行主动探测与感知。尚处于起步阶段的动态网络主动安全防御的创新技术研究任重而道远。

关键词: 被动防御;未知攻击;主动防御

Abstract: Dynamic network proactive security defence is an effective method for solving the unknown vulnerabilities and back door attacks in the information system. In this paper, the evolution defense mechanism (EDM) is proposed. According to the security status, network system security needs, EDM can select the best network configuration change elements to deal with potential attacks and ensure the safety requirements of a specific level. Dynamic reconfiguration and changes of the network need to be considered in accordance with the security situation of the system and the possible network attacks. The key is how to detect and the security situation and network attacks. It proposes that study on dynamic network proactive security defense in China is in the initial stage, and there is still much work to do.

Key words: passive defense; unknown attack; proactive defense

吴春明/WU Chunming
(浙江大学 计算机系统结构与网络安全研究所,浙江 杭州 310027)
(Institute of Computer System and Network Security, Zhejiang University, Hangzhou 310027, China)

- 动态网络主动安全防御技术已成为信息安全领域的重要研究方向
- 大数据中心、云平台等技术设施的出现,能使我们更有效地进行系统的数据采集、处理和分析
- 主动防御机制是对目前被动防御系统的拓展和补充,两者能够相辅相成

棱镜计划的曝光和斯诺登事件的持续发酵,表明了美国网络监控计划和针对中国物理隔离网络的威胁已穿透国门直逼我们面前,以“物理隔离”为基础的最后一道防线不复存在。

传统的网络安全防御思想是在现有网络体系架构的基础上建立包括防火墙和安全网关、入侵检测、病毒查杀、访问控制、数据加密等多层次的防御体系来提升网络及其应用的安全性。但近年来不断被披露的网络安全事件及由此带来的严重后果也逐渐暴露了传统的网络安全防御技术存在的问题,尤其是难以有效抵御系统未知软硬件漏洞的攻击,难以防御潜在的各类后门攻击,难以有效应对各类越来越复杂和智能化的渗透式网络入侵。近年来,研究动态网络主动安全防御技术已成为信息安全领域的重要方向。

如何通过动态化、随机化、主动化的手段改变网络信息系统的运行或执行环境,突破传统网络信息安全被动防御的窘境,将“亡羊补牢”式的被动防御转变为难以被侦测的主动防御是一种值得我们思考的创新思路[1-3]。

中国作为信息技术后进国家,关键领域的信息基础设施或装备几乎都被西方寡头公司控制,绝大部分核心元器件、高端芯片、基础/工具软件和半导体制程装备也都严重依赖进口。中国网络空间几乎单向透明地呈现在以美国为首的西方发达国家面前,信息安全面临极大威胁。当前,网络空间的软件攻击技术发展迅速,且已进入自动化程度高、攻击速度快、攻击工具复杂、潜伏更趋隐蔽的高级阶段。集成电路设计、制造、封装、测试和工具软件等环节被全球少数寡头企业垄断,在硬件或物理电路中植入或预留后门/陷阱成为新的攻击手段,且难以检测和有效防范。正在兴起的软硬件和电磁协同攻击技术具有植入更隐蔽、识别更困难、

收稿日期:2015-11-20
网络出版时间:2015-12-28

隔离效果差、清理代价高等综合优势，正在成为主流攻击模式，给安全风险的评估、检测和防御都带来了前所未有的挑战，甚至作为防御方底线的加密手段也很难保证其最终的有效性，现有网络空间安全手段的匮乏已严重危及国家主权和社会安定。

在全球经济一体化、专业分工国际化的时代背景下，任何一个国家都不可能完全掌控包含设计链、生产链和供应链在内的完整的安全链。从理论上讲，目前软硬件设计中的漏洞又是不可避免的，即使中国自主设计的芯片、硬件和软件，迄今尚无有效的漏洞检测手段和杜绝方法，从工程科学的角度也很难证明在整个安全链诸环节中没有漏洞、或未被植入病毒木马和预留后门。而近年来，控制系统安全事故频发，中国工业安全也受到了严重威胁，已引起了各国政府和学术界的广泛关注[4]。

动态网络主动安全防御以提供运行环境的动态性、非确定性、异构性、非持续性为目的，通过网络系统中的环境、软件、数据等主动重构或迁移实现动态环境，以防御者可控的方式进行主动变化，对攻击者则表现为难以观察和预测的动态目标，从而大幅增加攻击难度和成本，大幅降低系统安全风险[5]。

文章从多个方面论述了我们对动态网络主动安全防御技术的一些思考和目前所做工作。

1 动态网络的主动变迁技术

安全这个话题，多年来是从防护、抵御外界的入侵、攻击的角度来谈论的，但由于目前防御和攻击之间的不对称，因此一旦遭到无所不在的攻击后，能主动招架、有效抵抗的可能性就变得很小。据此形态，我们可以从另外一个角度来看待这个问题：即利用网络的基础设施、传输协议、数据访问等能力来完成特定的某项任务，在执行任务过程中有效保护好各环节的动作或操作，对注入、驻留、渗透的攻击所需感知或匹配的网络环境进行动态变换，以切断攻击行为过程中的先验知识链（即在平时的攻防僵持状态，双方保持静态化）；因没有实质性的行为发生，此时的威胁是可容忍的；在访问、请求等功能或操作启动后即可发起动态变换的指令，配置成与静态化对峙时刻不同的网络状态，增加入侵攻击的难度；一旦任务结束即可释放各类资源，形成机动网络的生成、配置、执行与释放卸载的动态化机制[6]。

为了增强网络动态变化的随机性，可以增加部分冗余网络节点设备和链路，在不同时刻根据不同需求将其随机激活或休眠，以动态重构网络，从而使得整个网络难以被探测。

通过网络与配置的动态化，将静态的网络变成动态、随机可重构的网络，改变目前网络攻防双方不对称的状况，使攻击者无法有效确定攻击目标，从而实现动态的网络安全。

动态网络的主动重构防御的指导思想是：在保障网络服务、功能等价的前提下，利用网络可重构的技术手段，构建具有依据任务需求、主动变迁网络运行与传输环境的网络架构，通过对破坏网络攻击链的方法及措施的研究和设计，提高网络攻击难度，形成主动网络防御的能力。

动态网络的主动变迁需要在考虑现有网络基础设施组成结构的基础上，结合拓扑结构、路由、环境、软件等网络要素来考虑，其关键技术、变迁策略和协同机制可关注如下几个方面：

（1）潜伏部分网络物理节点设备。通过潜伏部分网络设备，在必要时将其激活，重构出一个网络，在不同时刻或者根据不同需求，可以激活不同的潜伏设备或休眠部分设备，从而增强探测整个网络结构的难度。

（2）按需动态生成逻辑服务网络。逻辑服务网络是按需动态生成和释放的，即使对同一用户提出的需求，在不同时段所生成的逻辑服务网络拓扑结构、映射到的物理设备位置、逻辑设备地址等都有可能不一样。因此，多样化变换的逻辑服务网络使得网络结构也更难以被探测，数据难以被追踪[7]。此外，同一物理设备内各逻辑设备间的隔离化处理，也可以有效降低诸如路由器分布式拒绝服务（DDos）攻击的危害。

（3）多样化、差异化的网络服务。通过构建逻辑服务网的方式为不同业务提供不同等级的安全传输服务，高效地重构、利用网络资源。

（4）多径、动态路由。通过动态路由，用户信息每次传输路径都可能不同，使得难以被追踪定位[8]；通过多径路由，用户信息在不同的路径上传输，即使部分信息被截获，窃听者也很难获得完整的信息。另外，通过域间/内虚拟路由技术、域间/内路由代理技术等也不失为可进一步拓展的手段。

（5）网络设备的“白盒”设计。将网络设备封闭结构下不同部件的松耦合，比如软件定义网络（SDN）实现的数据面、控制面和应用软件的分离，而可重构网络则基于开放标准的构件化设计思想，实现粒度可伸缩的弹性模块化，从而提高设备主动避免干扰的能力。

（6）IP地址的可变。通过IP地址变换，可达到资源在IP层面的动态变化，使网络扫描攻击环节失效，从而形成对后续网络攻击失去有效目标的有利局面，减缓网络中蠕虫、病毒和木马的转播[9]。

（7）SDN的控制器联动。可以考虑新型网络操作系统，采用多控制器联动、协同与虚拟配置，重构虚拟网络与虚拟机等的方式进行协同化变迁控制单元与组件。

在前期的研究工作中我们将生物启发方法[10]用于主动网络安全机制中，并且提出了演进防御机制（EDM）[11]。该机制根据网络系统安全状态、网络系统安全需求、用户特定应用的安全需求，选择最佳的网络

配置变化元素组合来应对潜在的攻击、保证特定等级的安全要求。通过结合目前SDN最新控制器技术，EDM架构的愿景可设为：保证多种动态网络配置变化元素种类的共存，避免在配置变化过程中的冲突，并充分利用SDN所具有的良好的可编程性，通过不断更新动态网络配置元素种类、更趋有效的网络配置动变策略来应对新的威胁，从而保证EDM的不断持续演进，提高处理威胁的效果、增强安全增益。同时，EDM架构的设计考虑了动态网络配置所带来的网络效能损失问题，使其能够根据网络实际特点来选择适合的动态网络配置组合策略，因而具有自适应网络环境的特性。在原理验证用例中同时实现了IP地址与数据流路径随机化变化机制，并实现了两种随机化机制的协同与冲突避免。

2 动态网络安全态势和网络攻击的感知

动态网络主动安全防御能有效防御未知漏洞和后门攻击，实现动态的网络安全，但需要考虑主动防御的代价。过于频繁的动态变化网络元素，则从安全代价权衡而言，可能是昂贵的。因此，网络的动态重构和变迁需要根据系统的安全态势和可能遭受的网络攻击来考虑，其关键是如何有效对系统的安全态势和网络的攻击进行主动探测与感知。

（1）多维数据和全局性能指标综合下的安全态势感知

可以通过在网络的各个关键节点处（包括安全防护设备、流量采集设备、关键资源服务器、交换路由设备等）部署传感器或通过数据采集接口，实时采集各节点的运行数据，包括系统告警、资源占用等，将其发送到系统的全局监控中心，进行实时分析、感知系统的当前安全态势[12]。

目前，大数据中心、云平台等技术设施的出现，一方面提高了系统的计算能力和存储能力，另一方面也能使我们可更有效地进行系统的自动化数据采集。这一点在目前的SDN和软件定义安全（SDS）[13]系统中更为突出。在SDN和SDS系统中，管控系统拥有全局视图和知识库，开放和标准化的安全接口，可协同安全设备联动，可对网络流量、网络行为、安全事件等进行自动化、全面的采集、分析。如果能通过大数据多维分析，从全局角度对威胁进行有效分析建模，则系统可根据所建立的模型有效感知系统安全态势，从而进行针对性的主动防御，增加入侵攻击的难度，提高系统的安全性[14]。

（2）利用伪装、诱骗等手段进行搅局

利用伪装、诱骗等手段，使入侵者无法得到真实的系统信息等先验知识，诱骗入侵者攻击一些预先设置的陷阱蜜罐系统，来发现入侵[15]。

- 指纹伪装和隐藏。将真实系统的指纹信息按照定制策略进行改变，返回“真真假假，虚虚实实”的系统信息，使入侵者无法确定系统的真实版本等信息，无从下手。并进行指纹伪装，返回一些不存在的漏洞信息，主动“引狼入室”，当入侵者上当后按照虚假的指纹信息进行相关攻击，系统可以及时发现，达到早期主动发现入侵的目的。
- 蜜罐防御。网络通信中攻击与防御的问题可视为博弈问题，可在传统蜜罐基础上通过使用模拟服务环境的保护色机制和模拟蜜罐特征的警戒色机制这些主动欺骗技术，使攻击者无法区分蜜罐和实际生产系统，从而达到对攻击者的有效迷惑和诱骗[16-17]。蜜罐的保护色技术是指蜜罐通过模仿周边运行环境和拟保护的生产系统特征，使攻击者无法识别蜜罐的存在。蜜罐的警戒色机制则是指生产系统模仿蜜罐，使得攻击者将系统识别为蜜罐而躲避攻击。

蜜罐防护是攻防双方参与的理性、非合作的诱骗过程，双方策略相互依存，都期望保护自身信息并获得对方信息以达到收益最大化，是一种非合作不完全信息动态博弈[18]。从攻击者视角看，对手不只是提供真实服务的生产系统，而是“蜜罐”和“伪蜜罐”；从防御者视角看，对手则包含合法用户和攻击者。

（3）利用动态的异构冗余机制主动感知网络的攻击

使用多个异构冗余的功能一致体同时运行同一请求，对响应结果进行择多表决，输出正确结果，及时发现网络攻击踪迹，报警异常信息。主动防御网络的动态异构冗余机制可以在不影响系统正常运行的情况下，高准确率下快速发现被入侵部件，并进行系统清洗和恢复。

动态的异构冗余主动防御机制需要解决两个关键问题：

- 异构冗余部件资源池的构建。为了便于进行系统清洗和恢复，可利用虚拟计算技术来构建异构冗余部件资源池[19]。资源池的部件提供相同的服务，但应用程序、操作系统、硬件等需存在差异，以减小异构平台服务器共模故障发生的可能性。
- 部件的选择调度及异常部件的清洗与恢复。可利用综合管控平台按照预定策略完成虚拟机池中虚拟机启动、清洗等调度工作，并且根据管控中心下发的异常部件服务信息执行查杀清洗。周期性或基于事件驱动等策略调度异构部件服务，调度标准是保证系统的功能集不变和尽可能减小系统漏洞交集的关键。

3 主被动防御的组合联动

主动防御机制不是摒弃目前的被动防御系统，不是不需要目前已有的被动防御技术和相关基础设施，而是对目前被动防御系统的拓展、深入和提升，两者之间绝不矛盾，而是相辅相成[20]。

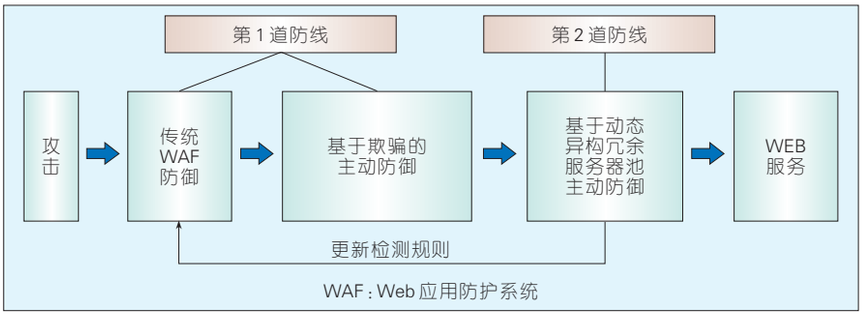
通常来说，可以利用传统的被动防御作为第1道防御阵线，解决大部分目前已知的网络攻击手段的防御问题；利用主动防御作为第2道防

线，解决未知漏洞和后门的防御问题，当然也可部署在第1道防线中。在主动防御发现入侵攻击时，可通过所记录的入侵攻击轨迹进行学习，得到新入侵攻击的特征，对被动防御的特征库和检测规则进行智能更新。被动防御可以利用现有的高效检测机制在入侵到达第2道阵线前过滤掉大部分攻击，主动防御则有效检测第1道防线无法防御的未知攻击，即挡住第1道防线的“漏网之鱼[21]”。

目前，在已开展的面向web应用的主动防御关键技术研究中，我们对主被动联合协作防御技术进行了有效尝试。如图1所示，首先利用已有的Web应用防护系统（WAF）防御大多数已知攻击，利用欺骗伪装技术实现指纹伪装、统一资源定位器（URL）跳变、虚拟蜜罐欺骗、敏感信息过滤、页面信息加扰和头部字段混淆，再利用动态异构冗余机制实现异构冗余体的动态调度、攻击入侵的主动感知和异常部件的有效清洗与恢复。通过上述主被动联合协作防御，不仅实现了web应用已知漏洞防御，而且通过动态变化、欺骗与清洗，可将多个静态的“带毒含菌”web服务应用进行结合，形成了一个动态随机的安全web服务系统。

4 结束语

在当前经济发展的大环境下，如何在保障中国经济快速发展同时做到信息安全的有效防护，是当前学术界与产业界亟需共同解决的一个重大课题。动态网络主动安全防御是解决信息系统中未知漏洞与后门攻击的有效手段，在主动防御系统中，我们不惧怕部件的“带毒含菌”，做到系统总体的安全风险主动可控，可缓解自主产业能力不足的困境，对于改变中国目前甚至今后相当长时期内，特别是在自主可控领域面临的严峻形势下，中国网络安全防御的被动局面具有重要的战略意义和巨大的应用价值。文章介绍了对动态网络主动安全防御技术的若干思考和一些工作，目前中国对相关技术的研究处于起步阶段，所做理论基础研究和相关实践并不充分，动态网络主动安全防御技术的研究任重而道远。



▲图1 主被动联合协作防御的web服务解决方案

参考文献
[1] 邬江兴, 张帆, 罗兴国, 等. 拟态计算与拟态安全防御[J]. 计算机学会通讯, 2015, 11(1): 8–14
[2] 邬江兴. 网络空间拟态安全防御[J]. 保密科学技术, 2014, 10(1): 4–9
[3] 邬江兴. 专题导读——拟态计算与拟态安全防御的原意和愿景[J]. 电信科学, 2014, 30(7): 1–7
[4] 马明杰, 孙奉刚, 翟立东, 等. 网络安全新威胁下我国面临的安全挑战和对策建议[J]. 电信科学, 2014, 30(7): 8–12
[5] COLBAUGH R, GLASS K. Proactive Defense for Evolving Cyber Threats [C]//2011 IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, China, 2011: 125–130
[6] 姜伟, 方滨兴, 田志宏, 等. 基于攻防随机博弈模型的防御策略选取研究[J]. 计算机研究与发展, 2015, 47(10): 1714–1723
[7] 梁宁宁, 兰巨龙, 程国振, 等. 基于拍卖博弈的可重构服务承载网动态构建算法 [J]. 电信科学, 2015, 31(5): 1–6. doi: 10.11959/j.issn.1000–0801.2015106
[8] CHUANG I, SU W T, KUO Y H. Secure Dynamic Routing Protocols Based on Cross–Layer Network Security Evaluation[C]// 2012 IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), Sydney, NSW, 2012: 303–308.doi: 10.1109/PIMRC.2012.6362800
[9] 田永春, 刘杰, 隋天宇. 军用无线网络动态安全防御技术研究[J]. 通信技术, 2015, 48(7): 830–834
[10] BALASUBRAMANIAM S, LEIBNITZ K, LIO P, et al. Biological Principles for Future Internet Architecture Design [J]. Communications Magazine, IEEE, 2011, 49 (7): 44–52. doi: 10.1109/MCOM.2011.5936154
[11] ZHOU H, WU C, JIANG M, et al. Evolving Defense Mechanism for Future Network Security [J]. Communications Magazine, IEEE, 2015, 53(4): 45–51. doi: 10.1109/MCOM.2015.7081074
[12] 韦勇, 连一峰, 冯登国. 基于信息融合的网络安全态势评估模型[J]. 计算机研究与发展, 2015, 46(3): 353–362
[13] ALA’ DARABSEH M A A, JARARWEH Y, BENKHELIFA E, et al. SDSecurity: A Software Defined Security Experimental Framework [C]// Third Workshop on Cloud Computing Systems, Networks, and Applications (CCSNA– 2015), London, UK, 2015
[14] SHI L, JIANG L, LIU D, et al. Mimicry Honeypots: A Brief Introduction [C] // Networking and Mobile Computing (WiCOM), 2012 8th International Conference on Wireless Communications, Shanghai, China, 2012: 1– 4. doi: 10.1109/WiCOM.2012.6478572
[15] 付钰, 陈永强, 吴晓平, 等. 基于随机博弈模型的网络攻防策略选取[J]. 北京邮电大学学报, 2014, 37(s1): 35–39
[16] 石乐义, 姜蓝蓝, 刘昕, 等. 拟态式蜜罐诱骗特性的博弈理论分析[J]. 电子与信息学报, 2013, 35(5): 1063–1068
[17] 石乐义, 姜蓝蓝, 贾春福, 等. 拟态式蜜罐诱骗特性的博弈理论分析[J]. 电子与信息学报, 2013, 35(5): 1420–1424
[18] FEINBERG Y. Strategic Communication [C]// Proceedings of the 13th Conference on Theoretical Aspects of Rationality and Knowledge, 2011: 1–11
[19] 张翔, 霍志刚, 马捷, 等. 虚拟机快速全系统在线迁移[J]. 计算机研究与发展, 2015, 49(3): 661–668
[20] LIN F Y S, WANG Y S, HUANG M Y. Effective Proactive and Reactive Defense Strategies Against Malicious Attacks in a Virtualized Honeynet [J]. Journal of Applied Mathematics, 2013
[21] 陈锋, 刘德辉, 张怡, 等. 基于威胁传播模型的层次化网络安全评估方法[J]. 计算机研究与发展, 2015, 48(6): 945–954

作者简介

吴春明，浙江大学计算机系统结构与网络安全研究所教授、博士生导师，国家“十二五”信息领域网络与通信技术主题专家组成员；主要研究方向为互联网体系结构、柔性可重构网络、网络资源弹性管控与虚拟化、网络试验床、网络安全主动防御等；曾主持、参加二十余项“973”、“863”、国家自然科学基金、国家科技基础条件平台等项目的研发工作；已发表SCI/EI论文80余篇，授权及申请国家发明专利20余项，出版著作2部。