doi:10.3772/j.issn.1002-0470.2017.08.002

通信网络动目标防御技术研究①

向 征②* 谭田天③** 蔡桂林*** 王小峰** 罗跃斌**

(*湖南信息学院信息中心 长沙 410073)

(**国防科技大学计算机学院 长沙 410073)

(***中国人民解放军 95942 部队 武汉 430313)

摘 要 论述了通信网络动目标防御(MTD)概念,从攻击面特征及动目标防御功能性内涵的角度,对现有动目标防御技术进行了归类和分析。在现有研究的基础上设计了基于端信息跳变的动目标防御系统,并对其抗攻击性能进行了分析。该系统能通过通信过程中持续变化攻击面增大攻击成本、复杂度和降低攻击成功率,从根本上提高防御攻击的性能。该研究可为多机制结合的动目标防御系统的设计与实现提供理论基础。

关键词 通信网络安全, 动目标防御(MTD), 综述, 主动防御, 变换机制

0 引 言

现有通信网络特征的静态性及通信应用、通信协议的单一性,为攻击者提供了充足的时间和便利,现有防御机制主要包括从消除 bug、识别攻击代码、下发补丁或从感染症状入手等,效果均有限, 为改变通信防御者的劣势被动地位,提升通信设备、应用等的抗攻击能力和弹性,美国国防研究人员提出了动目标防御(moving target defense, MTD)技术。目前国内学术界系统性分析介绍动目标防御技术的文献很少,本文从相关概念及发展战略出发,重点对现有移动目标防御技术研究进行归类与分析,研究动目标防御机制及其最新进展,为多机制结合的动目标防御的提出、设计与实现奠定理论基础。

1 相关概念

动目标防御研究中的基本核心概念主要有4个: 攻击面、攻击面变换、动目标以及动目标防御。

1.1 攻击面

系统攻击面的概念由 Manadhata[1] 等正式提出,将单个系统的攻击面定义为攻击者可进入系统并造成潜在威胁的方法集合;Zhu[2] 等将攻击面定义为系统外显的可能会被攻击者利用的脆弱性集合;Wei 等将云服务中一个活性虚拟机实例的攻击面定义为其外显的可用资源的总额[3]; Zhuang 等认为系统攻击面由暴露在攻击者面前的系统资源及已被侵害的可用来进入系统的网络资源共同组成[4]。

1.2 动目标及动目标防御

美国国防安全委员会报告[5] 中提出动目标是可在多个维度移动以降低攻击者优势并增加弹性的系统。2010 年发布的《网络安全游戏规则的研究与发展建议》[6] 中对动目标防御特征描述为:以内部可管理的方式持续改变一个或多个系统属性,使目标攻击面在攻击者面前呈现出一种不可预测性,从而降低攻击者成功 攻击的概率。

本研究认为,动目标防御功能性内涵应包括目

① 863 计划(2011AA01A103),高等学校博士学科点专项科研基金(20114307110006),长江学者和创新团队发展计划(IRT1012)和信息保障技术重点实验室开放基金(KJ-12-07)资助项目。

② 男,1979 年生;研究方向:网络安全。

③ 通讯作者,E-mail: happinesschild@126.com

(收稿日期:2017-04-06)

标的变化性、变化的可管理性、变化的持续性、变化的快速性以及变化的多样性五个方面,如表 1 所示。其中目标的变化性是动目标防御技术的关键,所有通过攻击面变换以实现通信系统中被保护目标不可预测的技术都可归类为动目标防御技术[7,8]。

表 1　动目标防御功能性内涵

功能特性	内涵
目标的变化性	被保护目标“移动”起来,改变现有通信网络配 置及特征造成的易攻难守
变化的可管理性	攻击面变换必须有良好的内部可管理性,保证任务的连续性及系统的功能与性能。
变化的持续性	降低攻击所依赖的静态性,提高攻击的复杂性
变化的快速性	在通信攻防军备竞赛中领先,让攻击者收集的信 息或发起的攻击快速失效
变化的多样性	变换方式的多样,攻击面参数值域的多样,多个 维度提高系统安全性与弹性。

2　动目标防御技术机制分析

依据执行栈中的位置层次,本文将现有动目标技术分为动态通信网络、动态通信运行环境、动态通信应用及动态数据四个大类(图 1)。

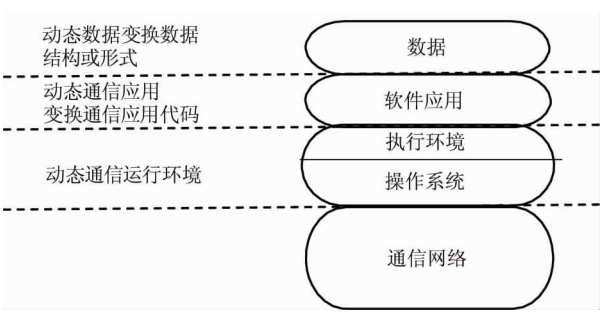


图 1　动目标防御机制分类

2.1　动态通信网络

动态通信网络机制通过端到端通信的双方或一方按照协定改变端口、地址、时隙、加密算法甚至协议等信息,破坏攻击者的攻击和对抗干扰,实现网络的动态变化,使攻击者无法通过常规 手段收集有效信息或收集的有效信息迅速失效,增加攻击代价及复杂度,有效抑制攻击的影响范围。

2.1.1　基于端信息计算的变化机制

基于端信息计算的变化机制是通过通信一方或双方利用己端的已知信息(地址、端口、密钥、时间等)计算下一步的连接信息。

(1) 动态网络地址变换

动态网络地址变换(dynamic network address translation,DYNAT)[9]通过变化报文头中主机标识信息来防御网络嗅探攻击。路由前,通过 DYNAT-shim 对报文头中发送方端口和地址进行转换,转换算法依赖于预先设定好的随时间变化的参数,DYNAT gateway 逆转换报文头域获取初始身份信息,处理后发送给接收方。该机制被设计来保护部署在集中式网关后的静态节点,对用户不透明,且 DYNAT gateway 压力较大,网络配置动态性较高时,可能会出现节点同步失效。

(2) 移动目标 IPv6 防御

移动目标 IPv6 防御(moving target IPv6 defense,MT6D)[10]是 IPv6 网络层动目标防御方法。通信双方利用各自当前地 址的接口标识符(interface identifier,IID)、一个共 享对称性密钥以及系统时间,计算出下一步要使用 的接口标识符并通告,然后使用新的接口标识符通信。

通信双方 IPv6 地址的持续丰富变化,增加了攻击代价和困难度。但在同一时刻,路由器要为一个节点保存多个地址及相应对应关系,增加了存储开销。

2.1.2　基于随机的变化机制

基于随机的变化机制通过为端主机分配随机生成的 IP 地址,实现网络地址动态变化。

(1) IP 地址变换

OpenFlow 随机主机变换(OpenFlow random host mutation,OF-RHM)及随机主机变换(random host mutation,RHM)[11,12]是由 Al-Shaer 等人提出的虚拟地址随机变换技术。OF-RHM 应用于 SDN 网络,通过 OpenFlow 控制器 频繁地为主机分配随机虚拟 IP,由 OF-switch 执行真实 IP 与虚拟 IP 的转换。OF-RHM 网络结构见图 2。

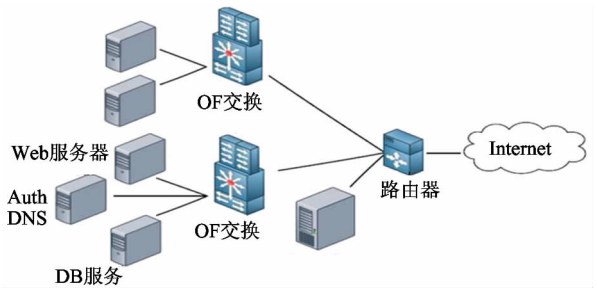


图 2 OF-RHM 网络结构

应用于传统通信网络的 RHM 使用低频变换(low frequency mutation, LFM) 和高频变换(high frequency mutation,HFM)实现虚拟 IP 的 分配,一个低频变换间隔区间内包含多个高频变换 间隔区间。每个低频变换间隔内,系统为每个主机 选择一个满足条件的随机地址范围,在每个高频变 换间隔内,在地址范围内随机选择一个虚拟 IP 分配 给主机。其不足是实施复杂度较高。

(2)网络地址空间随机化

网络地址空间随机化(network address space randomization,NASR)[13]通过在通信网络地址动态分配的环境中调节局域网节点 IP 地址的更改频率来防御蠕虫攻击。该机制需要配置动态主机配置协议(dynamic host configuration protocol, DHCP)服务器在不同时间间隔内终止 DHCP 租约(lease)以实现地址随机化。其不足是 需要修改对端主机的操作系统,且会导致端节点处活动连接的中断,因此部署代价比较高。

2.1.3 基于跳变的变化机制

基于跳变的变化机制主要通过跳变函数实现。

服务端连接信息的持续动态变化,使攻击者无法得知当前有效的服务端连接信息,从而增加攻击代价和复杂性,控制攻击的范围及影响。

(1) 通信端口跳变

Lee 等提出采用以系统时间、服务器与用户间共享私钥为变量的跳变函数来进行 UDP/TCP 端口跳变[14]。该技术兼容现有协议,不需要改变 Internet 基础设施,易于实施,简化了对恶意报文的检测和过滤,但严格时间同步机制在延时和拥塞环境下适用性较低。

Badishi 等提出了一种基于端口的配给信道防御机制[15],不同信道具有不同端口,不同时刻每个信道使用的端口也不同。端口由伪随机函数PRF*在最近使用过的端口集合中跳变选择。该机制将新选的端口信息随 ACK 报文传播以实现信息同步,存在端口信息被截获该泄漏的隐患。

(2) 通信地址跳变

通信地址跳变(network address hopping)[16]通过多个信道的数据连接来传递一个通信会话的数据流。该机制改变了两个通信体之间的通信模式,跳变序列信息明文通过服务器对用户的初始响应报文(如 TCP SYN-ACK)来传输,存在报文传 输方式被截获该泄漏的隐患。

(3) 通信端口和地址跳变

APOD(application that participate in their own defense)项目[17]通过端口和地址同时跳变提供以通信网络为中心的防御以提高应用的弹性,但需要安装特定的客户端组件完成地址和端口号的 转换,部署 NAT 网关实现逆向映射,由于不改变实际地址和端口,无法防御内部攻击。

雷声公司的 MORPHINATOR (Morphing Network Assets to Restrict Adversarial Reconnaissance)项目[18]聚焦端口跳变和地址跳变技术,研制具有“变形”能力的计算机网络原型, 实现随时间变形以迷惑网络入侵者并阻止网络攻击。MORPHINATOR 中使用了网络机动,动态更改网络的方面(aspects)和配置(configuration), 使主机和应用变得不可检测和不可预测,以预防、延迟或阻止网络攻击,且依然具有良好的被管理性。

(4) 基于通信协议的变换机制

即使主机系统带有高度的多样性,攻击者仍可通过探索通信协议的脆弱性发起攻击,基于通信协议的变换机制可以防御针对特定通信协议漏洞的网络攻击,获得比单一固定协议更高的安全性和更好的扩展性。

协议跳跃覆盖信道(protocol hopping cover channels,PHCC)[19]通过改变已建立隧道的协议来实现隐蔽信道,需要预先选定一组备用协议(选择原则与协议是否正在 被使用无关),在两个节点进行通信过程中,或在某台设备内不同部件间传输数

据过程中随机跳变 或者依据预先定义的顺序跳变。

2.1.4　其它动态通信网络机制

(1) 自屏蔽动态通信网络结构

自屏蔽动态网络结构(self-shielding dynamic network architecture,SDNA)[20]互补结合现有通信网络技术、hypervisor 技术、基于 CAC 的认证技术以及 IPv6 等多种技术,改变网络形态以提高整体安全度,限制了攻击者信息收集和网络传播能力。但该结构要求报文到达目的地前至少穿过一个中间节点,且源节点需逐步建立安全通道,进行数据的认证传输, 开销较大且会对用户的网络操作造成影响。

(2) 基于诱骗的变化机制

Clark 等提出了基于诱骗的动目标防御 方法[21],通过在通信网络中引入大量带有合法 IP 地址和简化的通用通信协议的欺骗节点,随机化真实节点和欺骗节点的 IP 地址,降低真实节点被识别定位的概率。其不足是频繁的地址切换会影响通信性能,且部署大量虚节点会增加资源开销。

2.2　动态通信运行环境

动态通信运行环境机制是动态通信平台与动态执行环境的结合体,通过变换通信应用运行时所需执行环境(包括软硬件、操作系统、配置文件等),实现攻击面变换,控制攻击范围及影响。

2.2.1　动态通信平台

变换通信平台可抵御针对通信平台特征的攻击,包括变化操作系统、处理器结构、虚拟机实例、存储系统、通信信道和其他底层环境。动态通信平台技术可以在平台间迁移通信应用,或在关联平台执行相同的通信应用。

(1) 可信动态逻辑异构

可信动态逻辑异构(trusted dynamic logical heterogeneity,TDLH)系统是通过平台多样性来提高应用生存性的框架[22],允许随机时间间隔内运行中的通信应用保留状态(包括执行状态、打开的文件和网络连接)迁移到其它异构平台。为保证目标平台安全性,迁移前采用可信平台模块(trusted platform module,TPM)进行可信验证。

(2) 自我净化入侵容忍和移动攻击面

自我净化入侵容忍(self-cleansing intrusion tolerance,SCIT)[23]通过虚拟化技术创建多个初始状态相同的虚拟服务器以轮换方式提供相同服务,随机选择上线的虚拟服务器,按预定状态重置下线虚拟服务器。其不足是攻击者探测到虚拟机初始状态的脆弱点仍可 成功发起相应攻击。移动攻击面(moving attack surfaces,MAS)[24]是提供 web 服务的每个虚拟服务器都配置的唯一 的软件集合,多样化的攻击面成功弥补了 SCIT 的 不足。同时配置多个虚拟机提供同一服务,在极短 时间内轮换,资源冗余度较高,管理开销较大。

2.2.2　动态执行环境

动态执行环境机制通过通信平台配置、目标地址、指令集的不可预测来迷惑攻击者,增加攻击成本,且攻击方法无法简单移植,从而抑制了攻击范围。

(1) 地址空间随机化/入侵集随机化

地址空间随机化(address space randomization,ASR)通过随机化目标在 memory 中的位置信息,使依赖目标地址信息的攻击失效[1]。(instruction-set randomization,ISR)技术[25]通过对随机密钥对系统指令集加密处理,保护系统免遭代码注入攻击,但随机范围较小,存在被成功破解的可能。

(2) 变化计算机配置

John 等人提出对现有系统配置实施变化以获得更安全的配置[26,27]。该方法首先通过发现组件将系统配置编码为染色体,执行遗传算法,产生安全度更高的配置子代,并将该子代种群发送到实现组件,实现组件在一组虚拟机里实现该子代种群,评估组件使用扫描工具(如 Nessus)和预定评分规则对新群体安全性进行可行性评估,依据评估结果选择染色体送往发现组件进行新一轮进化,同 时选择合适的配置染色体部署到主机上。

2.3　动态通信应用

动态通信应用机制主要以软件为变化对象,对其实施各种变换技术,在攻击者面前呈现不可预测的目标,增加相应攻击难度,提高软件抗攻击能力。

2.3.1　多样化变换机制

通信应用的多样化变换主要通过不同方法产生多个功能等价,行为特性相异的变体交替运行, 使

系统攻击面呈现出丰富的变化,攻击难以移植,Jackson 等提出在编译器进行代码翻译时自动对机器代码进行多样化[28],对一般的安全需求自动产生唯一、功能等价的应用程序变体,大规模软件多样性使攻击困难度呈指数级增长;对较高的安全需求采用多变体执行环境(multi-variant execution environment,MVEE)同时运行多个程序变体,由监控代理检测,检测到攻击则立即关闭被害程序变 体,有效控制攻击影响。Christodorescu 等提出了一种通用的端到端软件多样化方法[29],对一个程序多次重复实施变换,不同应用多样化策略不 同。其不足是对应用的开发、部署和操作均有影响,实际部署代价较高。

2.3.2 等价变换机制

Rinard 认为现有软件系统的功能通常超出所需,不必要的功能引入了更多安全脆弱点。通 信应用的等价变换通过现有成熟技术,如输入校正(input rectification)、功能切除(functionality excision)、功能替换(functionality replacement)、循环穿孔(loop perforation)、循环内存分配(cyclic memory allocation)等,在满足需求的同时去除不必要功能,减小系统攻击面,但在系统遭受攻击时无法有效控制攻击范围及影响。

2.3.3 其他变换机制

螺旋式变结构屏蔽(helix metamorphic shield,HMS)[30]通过时空多样化引擎高速重置随机密钥对通信应用进行动态指令集随机化以实现攻击面变换,攻击被检测后生成事件指明脆弱性,触发修复引擎用进化算法产生进化变体,经过多样化变换后加以部署。该方法 在移动攻击面的同时不断修复攻击面,使通信应用自动进化为脆弱性更少的变体,但引入了大量计 算、检测及修复开销。

2.4 动态数据

动态数据机制是对通信应用数据进行语义等效变换,以抵御非法使用或访问。

2.4.1 数据多样化

数据多样化(data diversity)[31]是通过通信应用的每个变体运行语义等效数据,恶意输入导致的语义分歧可被变异监视器检测到。不同指令将每个变量地址和运行空间分开有助于 减轻依赖特定内存地址的注入攻击。其不足是攻击者仍可定位应用的数据部分,或使用同时影响所有变体的高级控制注入攻击。

2.4.2 数据随机化

现有数据随机化(data randomization,DR)[32]机制主要通过异或操作对不同数据对象进行随机化。Cowan 等提出将指针与随机化密钥异或后存入存储器中[33],待指针被载入寄存器时再将其还原以防御指针失效攻击;Cadar 等提出通过静态分析为指令操作数进行等价类划分,并为每个等价类分配随机掩码与相应数据进行异或操作[34]。攻击者进行与分析结果不同的访存会导致错误,从而抵御针对存储器错误所进行的探测攻击;Bhatkar 等提出在程序初始化时,分析程序所包含的所有数据类型,然后对每个数据对象选择唯一的随机数来实现异或加密,且仅在数据被引用时才进行解密,以抵御相对地址攻击[35]。

借鉴 MIT Lincoln laboratory 评估动目标防御所归纳的攻击链,本文对动态通信网络、动态通信 运行环境、动态通信应用、动态数据等 4 种动目标防御技术进行了分析,这 4 种机制在攻击链中的作用如表 2 所列。

表 2 四种机制在攻击链中的作用

MTD	攻击链				
	侦查	访问	开发	发动	持续
动态通信网络	+			+	
动态通信运行环境		+	+		+
动态通信应用			+	+	
动态数据			+	+	

3 主动防御系统设计及性能分析

基于跳变机制,设计了通信网络主动防护系统框架(图 3),通过伪随机跳变端口、地址、协议、服务时隙等端信息,使攻击者进行的拒绝服务等攻击难以实现,并以一定的可能性被诱骗至蜜罐主机, 采用加密算法的跳变使得截获到的数据报文难以排序及解密,情报搜集完成后即失效,大大增加了攻击者

的时间代价,提高了系统的可用性和机密性。如图所示。该系统以控制模块为核心,通过预警模块收集当前遭受的攻击信息,通过管理模块产生端信息跳变图案,任务切换模块按照控制模块指令对通信机、干扰机和蜜罐机进行通信、干扰、蜜罐等任务转换。

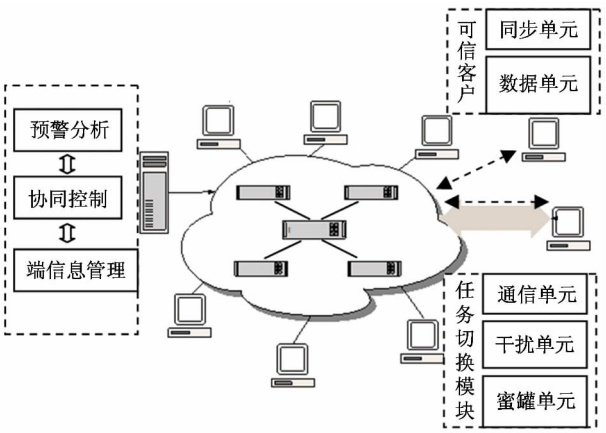


图 3　基于跳变机制的主动防御系统框架

假定攻击者获知端信息跳变策略发起进攻,由于任意时刻用于端信息跳变的跳变图案是唯一的,可推知攻击成功击时间为

$$T' = T(1 + \sum_{i=1}^{nmk-1} [\, i \frac{C_{nmk-1}^{i}}{C_{nmk}^{i} C_{nmk-i}^{1}}))) \tag{1}$$

其中,n 为可用跳变地址数,m 为端口数,k 为协议数,可用跳变图案数为 nmk。可见端信息跳 变大大增 加了攻击者的时间代价。

假定系统不可用阈值为连续时间 $T(T >> t)$,遭受的单位平均攻击强度 X 大于 X_T,则

$$X = \frac{r/s}{nmk} \tag{2}$$

时隙不可用概率 P_t 和系统稳态可用概率 P_{Avail} 为

$$P_t = p(X > Xt) = p(\frac{\frac{r}{s}}{nmk} > X_\tau) \tag{3}$$

$$P_{\text{Avail}} = 1 - \sum_{i=\tau/t}^{\infty} P_\tau^i = 1 - \frac{P_t^{\tau/t}}{1 - P_t} \tag{4}$$

其中,r 为 DoS 攻击者的攻击数据速率,s 为攻击报文大小,t 为平均跳变时隙。由此可见,跳 变图案 nmk 越多,单位平均攻击强度 X 就越小,单位平均攻击强度 X 越小或端信息跳变越快系统可用性就越好。

对于截获攻击,该系统通过端口、地址、协议、时隙的跳变,使得数据报文散布在背景数据噪声中,成功截获、重组、破译完整报文的概率为

$$P_S = (\frac{1}{P_{\lfloor N_0/S \rfloor + l}^{1} l})^k = \frac{1}{((\lfloor \frac{N_0}{S} \rfloor + 1) l)^k} \tag{5}$$

其中,l 为可用加密算法数,N_0 为背景噪声理想均匀的数据量,S 为有效报文数据量,k 为完整数据报文划分的段数。

由此可见,端信息跳变机制降低了攻击者的成功破译的概率,增加了时间代价,提高了系统的机密性。

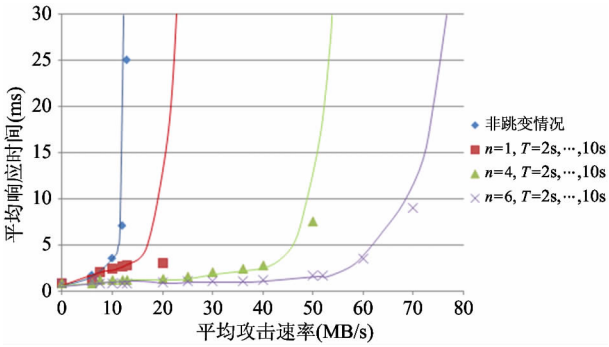
对该防御系统进行 SYN-Flood 攻击实验和截获攻击实验,实验环境配置见表 3,实验结果如图 4 所示。

表 3　抗 DoS 实验环境配置

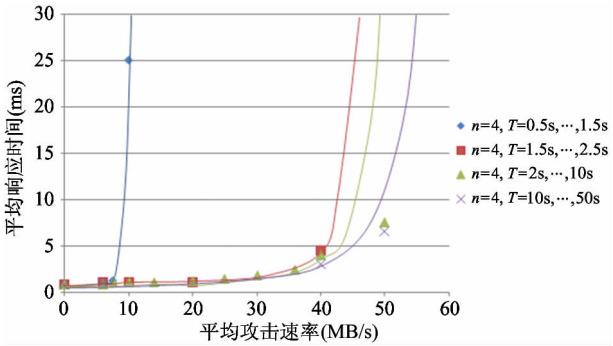
	控制机	同步机	服务机群	客户机	DoS 攻击机	截获攻击
带宽(MB/s)	100	100	100	100	1000	100
操作系统	Win-XP	Win-XP	Linux, Win-XP		Linux	Win-XP
工作方式	Agent 控制	UDP 服务	端信息跳变		SYN-Flood	Sniffing

从图 4(a)可以看出,对于抗 DoS,端信息跳变性能远优于传统服务和简单端口跳变服务,并与可用跳变地址数成正比,图 4(b)表明,过快的服务切换将导致性能下降。端信息跳变主动防御系统可大大提高系统抗 DoS 性能,但跳变速率应根据网络规模、拥塞程度等进行设置。

截获攻击实验选择了最有利于攻击者的设置,截获机位于共享 Hub 局域网中,无其他主机干扰,5 台服务器,6 台客户机。



（a）非跳变、端口跳变及不同地址数的端信息跳变



（b）不同跳变时隙影响端信息跳变

图 4　抗 DoS 攻击性能实验数据

实验结果如图 5 所示，相比非跳变与端口跳变，端信息跳变机制有效分散了网络流量，伪随机跳变加密算法大大增加了解密的复杂度。

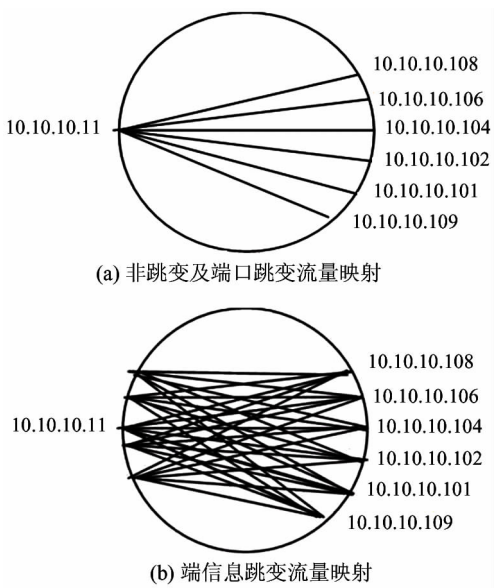


图 5　抗端信息跳变截获攻击数据

4　结　论

作为一项革命性的通信防御技术，动目标防御一经提出就受到了研究人员的高度关注。高质量的动目标防御系统迫切需要全面系统的机制理论指导，本文从攻击面特征及动目标防御功能性内涵出发，对现有动目标防御研究技术进行了归类与分析，系统地研究了动目标防御机制及其最新进展，设计了基于端信息跳变机制的主动防御系统，并从抗攻击性能进行了分析，为多机制结合的动目标防御的设计与实现奠定了理论基础。另外，动目标防御机制的变化机制与控制、动目标防御机制实用化与效能评估，以及如何结合动目标防御思想以提高传统静态防御方法效果也将成为未来通信防御的研究热点。

参考文献

[1] Manadhata P K, Wing J M. An attack surface metric. *IEEE Transactions on Software Engineering*, 2011, 37(3): 371-386

[2] Zhu Q, Başar T. Game-theoretic approach to feedback-driven multi-stage moving target defense. In: Proceedings of the 4th International Conference on Decision and Game Theory for Security, Fort Worth, USA, 2013. 246-263

[3] Wei P, Feng L, Chin-Tser H, et al. A moving-target defense strategy for Cloud-based services with heterogeneous and dynamic attack surfaces. In: Proceedings of IEEE International Conference on Communications, Sydney, Australia, 2014. 804-809

[4] Zhuang R, Zhang S, Deloach S A, et al. Simulation-based approaches to studying effectiveness of moving-target network defense. *National Symposiumon Moving Target Research*, 2013, 53(39): 15111-15126

[5] July. Cybersecurity Progress after President Obama's Address. The WhiteHouse National Security Council, 2012

[6] NITRD CSIA IWG. Cybersecurity Game-Change Research & Development Recommendations. NITRD, 2010

[7] Cai G L, Wang B S, Luo Y B, et al. Research and Development of moving target defense technology. *Journal of Computer Research and Development*, 2016, 53(5): 968-987

[8] Manadhata P. Game Theoretic Approaches to Attack Surface Shifting. New York: Springer, 2013. 1-13

[9] Kewley D, Fink R, Lowry J, et al. Dynamic approaches to thwart adversary intelligence gathering. In: Proceedings of the DARPA Information Survivability Conference & Exposition II, Anaheim, USA, 2001. 176-185

[10] Basam D, Ransbottom J S, Marchany R C, et al. Strengthening MT6D defenses with LXC-based honeypot capabilities. *Electricaland Computer Engineering*, 2016, (2):12

[11] Jafarian J H, Al-Shaer E, Duan Q. Adversary-aware IP address randomization for proactive agility against sophisticated attackers. In: Proceedings of 2015 IEEE Conference on Computer Communications (INFOCOM), Hong Kong, China, 2015. 738-746

[12] Jafar Haadi Jafarian, Al-Shaer E, Duan Q. An effective address mutation approach for disrupting reconnaissance attacks. *IEEE Transactions on Information Forensics and Security*, 2015, 10(12): 2562-2577

[13] Antonatos S, Akritidis P, Markatos E P, et al. Defending against hitlist worms using network address space randomization. In: Proceedings of the 2005 ACM Workshop on Rapid Malcode, Fairfax, USA, 2005. 30-40

[14] Lee H C, Thing V L L. Port hopping for resilient networks. In: Proceedings of 2004 IEEE 60th Vehicular Technology Conference, Los Angeles, USA, 2004. 3291-3295

[15] Badishi G, Herzberg A, Keidar I. Keeping denial of service attackers in the dark. *IEEE Transactions on Dependable & Secure Computing*, 2007, 4(3):191-204

[16] Sifalakis M, Schmid S, Hutchison D. Network address hopping: a mechanism to enhance data protection for packet communications. In: Proceedings of IEEE International Conference on Communications, Beijing, China, 2005. 1518-1523

[17] Atighetchi M, Pal P, Webber F, et al. Adaptive use of network-centric mechanisms in cyber-defense. In: Proceedings of IEEE International Symposium on Object-Oriented Real-Time Distributed Computing, Hokkaido, Japan, 2003. 183-192

[18] Raytheon Company. MORPHINATOR. http://www.raytheon.com/:Raytheon company, 2012

[19] Wendzel S. Protocol hopping covert channels. http://www.wendzel.de/dr.org/files/Papers/protocolhopping_MP_DE.pdf: Wendzel, 2008

[20] Yackoski J, Xie P, Bullen H, et al. A self-shielding dynamic network architecture. In: Proceedings of the Military Communications Conference, New York, USA, 2011. 1381-1386

[21] Clark A, Sun K, Poovendran R. Effectiveness of IP address randomization in decoy-based moving target defense. In: Proceedings of the Decision and Control, Florence, Italy, 2013. 678-685

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

[23] Bangalore A K, Sood A K. Securing web servers using self cleansing intrusion tolerance. In: Proceedings of the International Conference on Dependability, Brunow, Poland, 2009. 60-65

[24] Huang Y, Ghosh A. Introducing Diversity and Uncertainty to Create Moving Attack Surfaces for Web Services. New York: Springer, 2011, 54: 131-151

[25] Kc G S, Keromytis A D, Prevelakis V. Countering code-injection attacks with instruction-set randomization. In: Proceedings of ACM Conference on Computer and Communications Security, Washington, USA, 2003. 272-280

[26] Lucas B, Fulp E W, John D J, et al. An initial framework for evolving computer configurations as a moving target defense. In: Proceedings of the Cyber and Information Security Research Conference, New York, USA, 2014. 69-72

[27] John D J, Smith R W, Turkett W H, et al. Evolutionary based moving target cyber defense. In: Proceedings of the Companion Publication of the 2014 Annual Conference on Genetic and Evolutionary Computation, Vancouver, Canada, 2014. 1261-1268

[28] Jackson T, Salamat B, Homescu A, et al. Compiler-generated software diversity. *Advances in Information Security*, 2011, 54: 77-98

[29] Christodorescu M, Fredrikson M, Jha S, et al. End-to-End Software Diversification of Internet Services. New York: Springer, 2011, 54: 117-130

[30] Goues C, Nguyen-Tuong A, Chen H, et al. Moving Target Defenses in the Helix Self-Regenerative Architecture.

New York: Springer, 2013, 100:117-149

[31] Ma J, Dunagan J, Wang H J, et al. Finding diversity in remote code injection exploits. In: Proceedings of the 6th ACM SIGCOMM Conference on Internet measurement, Rio de Janeriro, Brazil, 2006. 53-64

[32] Bhatkar S, Sekar R. Data space randomization. In: Proceedings of the 5th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Paris, France, 2008. 1-22

[33] Cowan C, Beattie S, Johansen J, et al. PointGuard™: protecting pointers from buffer overflow vulnerabilities. In: Proceedings of the 12th Conference on USENIX Security Symposium, Washington, USA, 2003, 12:7

[34] Rinard M C, Cadar C, Dumitran D, et al. A dynamic technique for eliminating buffer overflow vulnerabilities (and other memory errors). In: Proceedings of the 20th Annual Computer Security Applications Conference, Tucson, USA, 2004. 82-90

[35] Bhatkar S, DuVarney D C, Sekar R. Address obfuscation: an efficient approach to combat a broad range of memory error exploits. In: Proceedings of the Conference on USENIX Security Symposium, Berkeley, USA, 2003. 105-120

Research on the moving target defense technology of communication networks

Xiang Zheng[*], Tan Tiantian[**], Cai Guilin[***], Wang Xiaofeng[**], Luo Yuebin[**]

([*] Information Centre, Hunan Institute of Information Technology, Changsha 410073)

([**] Department of Computer, National University of Defense Technology, Changsha 410073)

([***] Crop 95942, Wuhan 430313)

Abstract

The concept of moving target defense (MTD) of communication networks is interpreted, and the existing moving target defense techniques are classified and analyzed from the angles of attack surface feature and functional connotation of moving target defense. A moving target defense system based on end hopping is designed on the basis of the study of present techniques of moving target denfense, and its anti-attack performance is analyzed. The system increases the attack cost and complexity and decreases the attack sucess ratge by continually changing the attack surface, thus its attack defense performance can be radically improved. This study can provide the theoretical basis for design and implementation of multi-mechanism moving target defense systems.

Key words: communication network security, moving target defense (MTD), survey, active defense, shifting mechanism