**重庆邮电大学本科生堂下考试答卷**

**2020-2021学年第 1学期**

**课程名称：计算机网络**

**姓 名：姜岙**

**年 级：2018**

**学 号：2018211406**

**专 业：计算机科学与技术**

**2020年11月25日**

**网络层移动目标防御技术研究**

作者，姜岙

(重庆邮电大学)

**摘 要:** 移动目标防御是解决网络安全问题的新思想，是基于网络空间攻防成本严重不对称而提 出，通过动态变化防御目标对外呈现的攻击面，阻断或扰乱攻击所依赖的静态性、相似性和持 续性，以此挫败网络攻击。结合网络层移动目标防御技术的最新研究成果，提出网络层移动目 标防御系统，从而达到提高防御能力的目的。

**关键词：**网络安全; 移动目标防御; 网络层; 攻击面。

**Research on Network Layer Defense Technology Based on Moving Target Defense**

**SURNAME Name,JIANG AO**

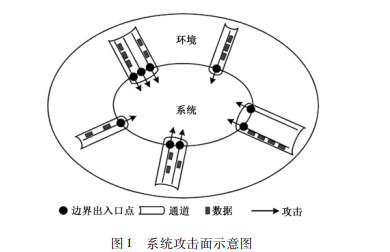
**Abstract:** As a new idea in addressing network security，mobile target defense is proposed based on the serious asymmetry of the cyberspace attack and defense cost． By dynamically changing the attack surface of the defense target，blocking or disrupting the static feature，similarity and persistence the attack relies on，the cyber attack is expected to be thus foiled． Based on the latest research results of network layer mobile target defense technology，this paper proposes a network layer mobile target defense system to improve the defense capabilities．

**Key words:** network security; moving target defense; network layer; attack surface.

**1 网络层移动目标防御研究现状**

移动目标防御( Moving Target Defense，MTD) 最早由美国提出，旨在改变网络空间攻防双方信息 不对称的不利局面，被称为“改变游戏规则”的网络安全研究新方向。移动目标防御的主要思 路是产生和部署多种不同类型的、动态变化的防护策略和机制，通过持续动态改变系统对外呈现的攻 击面，减少目标的静态性、相似性和确定性，降低安全漏洞被发现和利用的概率，以此迷惑攻击者，增 加攻击者的攻击成本和攻击难度。移动目标防御不是某一类具体的防御手段，而是一种安全防御指导思想。通过动态改变系统某些资源属性或属性对外呈现的攻击面，以此误导攻击者，使其无法准确定位攻击目标或攻击不正确目标的防护思路， 均属于移动目标防御的范畴。

移动目标防御通过动态改改变防护目标的攻击 面来阻断攻击。攻击面的概念最早由文献［5-6］提 出，是系统有可能被攻击者用于实施攻击的资源属性的集合，是攻击者入侵的通道，如系统的弱口令、 应用程序漏洞、静态配置的 IP 地址、开放的端口等。直观上看，某个系统的攻击面越大，其安全风 险越高，图 1 是系统攻击面的原理示意图。



**1．1 网络架构动态化**

可变网络( Mutable Networks，MUTE)在保持操作和服务完整性与连续性的同时，允许周期性 地随机改变网络配置( 称为变异) ，以保护网络免 受外部侦察和映射攻击，同时提高网络抵御 DDoS 攻击的能力。MUTE通过以下技术实现移动目标防御: ①随机地址跳变: 频繁地为网络主机随机分配 适配网卡地址的虚拟 IP 地址，这种虚拟 IP 地址被 独立地用于路由，虚拟 IP 的不可预知性通过随机密钥来保证。随机化的 IP 地址从保留网段的地址 区间或者预先设置的地址区间中选取，这一地址空间足够大，并且国家正在进行的 IPv6 战略实质上为随机化提供了更广阔的可用空间; ②随机指纹: 主机的应答信息会被截获并被透 明地修改以最大化系统行为的信息熵，同时给出错 误的操作系统和应用程序标识。如果没有操作系 统类型和( 或) 应用程序服务器的确切标识细节，远程入侵将是不可行的。有 2 种机制来随机外部系统响应，一种是截取并修改会话控制报文，如 TCP 的三次握手，用错误的平台或服务识别来欺骗攻击者; 另一种技术基于防火墙，通过对所有拒 绝数据包的正面响应来欺骗扫描者。 这两种技术的融合使 MUTE 可应对多种形式 的攻击。在 MUTE 跳变时当前活跃的会话将保持连接。类似的动态网络架构还有自屏蔽动态网络架构 ( Self-shielding Dynamic Network Architecture，SDNA) 、MOTAG 架构等。 文献基于软件定义网络( Software Defined Network，SDN) 实现网络架构的随机变化，首先通过 SDN 控制器获得当前网络的完整状态信息，然后按照相应的周期随机改变主机地址、网络路由等信息，同时根据当前网络状态和配置提取数据建模，对当前网络可能遭受的攻击和安全威胁进行评估。

**1．2 网络地址随机化**

动态网络地址转换( Dynamic Network Address Translation，DYNAT) ［15］通过修改数据包头部的地 址信息来抵御网络嗅探攻击，在数据包路由之前对 数据包的目的地址进行变换( 变换算法可逆且随 时间动态变化) ; 接收端 DYNAT 网关收到该数据 包后，先对数据包中的地址信息进行逆变换，然后 发送给真正的接收方。 文献基于 OpenFlow 控制器不断地为主 机分配虚拟 IP 地址，同时维护网卡地址与虚拟地 址的映射和转换关系，网络内部主机之间的通信均由虚拟 IP 完成，从而增加了攻击者探测主机网卡 真实地址的难度。 网络地址空间随机化( Network Address Space Ｒandomization，NASＲ)按照不同的时间间隔终 止 DHCP 租约来频繁修改主机获得的地址，以此 来抵御蠕虫病毒的攻击，地址的动态变化可以基于 定时器实现，也可以在节点重启时进行。 1．3 端信息跳变 端信息跳变是指端到端的通信过程中，通信实 体按照事先约定随机变化端口、地址、通信协议、加密算法等［18］，从而实现端到端通信的动态防御。 文献利用服务器和客户端之间维护的共 享私钥、系统时间构建端口跳变函数，对服务器和 客户端之间通信的 TCP /UDP 端口进行动态改变， 通过身份认证的用户由于掌握私钥，能计算出当前 服务器正在使用的端口，非授权用户则无法获悉服 务器当前正在使用的端口，因此能够抵御对服务器 的 DDoS 攻击和漏洞扫描，但该方法对服务器和客 户端的时间同步性要求非常高。文献基于 SDN 架构提出一种端信息和传 输路径同时跳变的通信机制: 网络层移动目标防御技术研究 441 活性，以及跳变通信双方的端信息和传输路径，使 通信数据包按照多条传输路径到达目的地，因此多个用户的通信数据实现了混合传输，使攻击者无法 准确定位单一用户的通信数据，从而有效增加了攻击者实施中间人攻击的难度。网络欺骗技术 网络欺骗技术是防御方为改变攻守不对称格 局而引入的一种防御新思路，其核心思想是通过扰 乱攻击者的认知，诱导攻击者采取有利于防御方的 行动，增加其实施攻击的代价，降低其攻击成功概率［21］。针对攻击链中的系统侦察环节，可将移动目标防御的动态变换思想与网络欺骗技术相结 合，有针对性地对攻击者进行网络、应用、终端和数据的欺骗，诱骗攻击者对其实施攻击，从而触发攻 击告警，在战术战法层面改变防御者被动的格局。真实服务器是一个数据库服务器，只开放了 1433 端口，而 3389、22、445 等高危敏 感端口虚假开放。当攻击者对目标服务器的虚假 开放端口进行访问时，攻击流量被虚假响应。通过 这样的操作，在真实服务器上构建一系列虚假高危敏感端口，大大降低了真实服务器漏洞信息被发现 的概率。 针对网络扫描及蠕虫病毒的传播特性，可引入网络切片隔离技术，主要用于阻止威胁在进入网络 内部后对其他网络节点的渗透。可通过把内网每 个节点定义为一个逻辑隔离的子网，将现有内网的 二层交换提升为网络切片隔离交换模式，内网每台 终端之间都被逻辑隔离，并且能够实时全流量的监 控内网通信。具体可通过修改网络内部主机的 DHCP 数据包来实现。当内部主机发起 DHCP 请求时，修改 DHCP 服务器响应包中分配给主机的 IP 地址，同时维护修改前和修改后 2 个 IP 地址的 对应关系，最终使得内部主机获得的 IP 地址被划分到不同的逻辑子网，然后利用网络功能虚拟化技 术为每一台内部主机所在的逻辑子网生成大量的 虚假节点，使得每一个逻辑子网中均只有一台真实 主机存在，有效隔断非法二层通讯。

**2 网络层移动目标防御系统**

本文设计的网络层移动目标防御系统架构如 图 5 所示，主要包括管理层、内核层、用户层和物理 层，其中管理层包括 CLI 模块、WEB 模块、日志处 理模块、XMSD 模块; 内核层包括 DHCP 模块、AＲP 模块、DNS 模块、TCP /UDP 模块、ICMP /GＲE 模块、 PPPOE 模块、动态变换控制模块和数据分析控制 模块; 用户层包括动作库、Bypass 模块、协议判断模 块和动态变换转发模块; 物理层主要是网络接口。 管理层中的 XMSD 模块为整个框架下系统调 用的中间接口，CLI/WEB 通过 XML 文件方式将数 据输送给 XMSD，XMSD 解析 XML 文件并队形对 应的系统调用。 DHCP 模块给系统内部主机分配 IP 地址并创 建主机信息表，包括开启 DHCP 模式和关闭 DHCP 模式。开启 DHCP 模式时，系统作为 DHCP 服务器给系统内部主机分配 rip，同时生成对应的 vip 和 wip 保存在系统上的主机信息表中; 关闭 DHCP 模 式时，表明在系统外部有一个 DHCP 服务器，系统 把系统内部主机的 DHCP 请求转发至系统外部的 DHCP 服务器，系统外部的 DHCP 服务器给主机分配 wip，系统给主机生成 rip 和 vip。 AＲP 模块处理系统内部主机探测假网关 mac 地址的 AＲP 数据包，处理真实网关探测系统内部主机 mac 地址的 AＲP 数据包，处理系统外部主机 探测系统内部主机 mac 地址的 AＲP 数据包，处理系统内部主机探测系统外部主机的 AＲP 数据包， 对访问虚假节点的 AＲP 请求包进行虚假响应。

**3 实验测试与分析**

本文根据上节的系统架构图实现了一个原型 系统，为了对本系统功能和防御效进行评估。 2 台主机接入系统后获得了真实 IP、虚拟 IP、 外网 IP、虚拟域名、MAC地址和网关 MAC: 网络层移动目标防御技术研究 443 些信息会动态变化，系统实现了网络架构动态化、地址随机化和端信息跳变，系统内主机根据这些信息进行网络通信。

**4 结束语**

本文针对网络层的移动目标防御技术开展研究，在介绍移动目标防御基本原理的基础上，对现 有的研究网络层移动目标防御的公开文献进行了分析，给出网络层移动目标防御系统的基本架构， 并通过理论和实验评估了该系统对网络扫描和蠕虫病毒的防御效果，结果表明网络层移动目标防御系统可以有效降低扫描者命中内部主机的概率，快速检测和控制扫描行为，并可以在实际网络中部署和使用。

**参考文献**

［1］ 杨林，于全． 动态赋能网络空间防御［M］． 北京: 人民 邮电出版社，2016: 103-108．

［2］ ZHANG X Y，LI Z H． Overview on moving target defense technology［J］． Communications Technology，2013，46( 6) : 111-113．

［3］ JAJODIA，SUSHIL，et al． Moving target defense: creating asymmetric uncertainty for cyber threats［M］． Springer Science ＆ Business Media，2011．

［4］ 蔡桂林，王宝生，王天佐，等． 移动目标防御技术研 究进展［J］． 计 算 机 研 究 与 发 展，2016，53 ( 5 ) : 968-987．

［5］ ZHU Q， BAT． Game-theoretic approach to feedback-driven multi-stage moving target defense［M］． Springer International Publishing，2013: 246-263．

［6］ PENG W，LI F，HUANG C-T，et al． A moving-target defense strategy for cloud-based services with heterogeneous and dynamic attack surfaces［C］/ /2014 IEEE International Conference on Communications， 2014: 804-809．