doi:10.1631/FITEE.1800516

题目：基于多维动态网络属性的新型企业网防御系统的设计与实现

概要：虽然周界安全模型在内部主机可靠时足够有效，但是随着企业采用移动和云技术，如自带设备（BYOD），该模型难以为继。有针对性的高级网络攻击通常采用网络杀伤链，例如，基于网络扫描技术收集潜在目标信息。本文提出一种“隔离和动态”网络防御方法，切断潜在杀伤链，降低攻击者收集信息的可用性。首先，通过网络隔离构建一个零信任网络环境，操纵多维网络属性跳变，使攻击者无法获得目标主机的特征和位置；其次，为企业网络提出一种基于软件定义的主动网络防御解决方案（SPD），并设计了一个通用框架，在不显著影响网络性能条件下，策略性地操纵 IP 地址、网络端口、域名和路径的协同跳变；然后，通过软件定义网络控制器（OpenDaylight）实现 SPD 概念验证系统；最后，搭建实验平台验证系统防扫描、防窃听和防拒绝服务（DoS）攻击的能力。结果表明，该系统可以显著降低网络侦察扫描信息的可用性，阻止网络窃听，并大幅增加攻击者的网络攻击成本。

关键词：企业网防御；软件定义网络；多维跳变