高等计算机网路

2020 年秋季学期

论文阅读 1

徐荣琛 2019214518 软件学院 2020 年 9 月 28 日

专题	路由协议安全
题目	On the Feasibility of Rerouting-based DDoS Defenses
作者	Tran M, Kang M S, Hsiao H C, et al.
会议	2019 IEEE Symposium on Security and Privacy

本篇论文的主要工作是论证了路由阻塞绕行技术（Routing Around Congestion，简称 RAC）在实际边界网关协议（BGP）中防御 DDoS 攻击的不可行性。

RAC 防御 DDoS 攻击的核心是目的自治系统利用 BGP 路由毒化机制，向关键流量源提供一条新的、不受洪泛攻击影响的路由旁路。例如在图 1中，目的自治系统 D 为了排除攻击受影响 W 相关路由通路，并向关键流量源 C 提供新的路由旁路 CXYZD，于是向临近的自治系统 Z 发布包含毒化 W 的路由更新指令，随后网络逐步更新并收敛，C 到 D 的路由通路即从原来的 CXWZD 迁移到了 CXYZD。

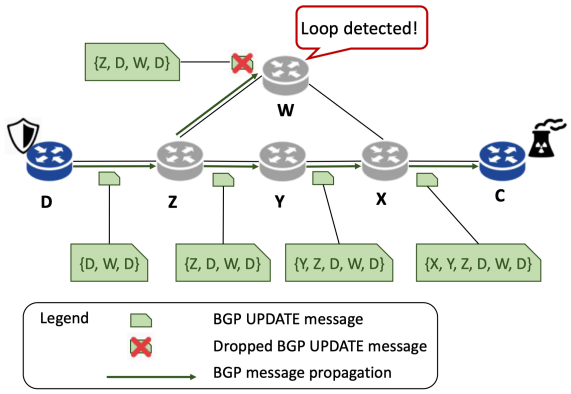

图 1: RAC 防御示意图

虽然上述的 RAC 防御模式在理论上是可行的，但是本论文从实际 Internet 应用的角度论证了在现实中该技术方案的不可行性，不可行的原因文章从以下几个方面进行了论述：

- 在实际应用之中，如果要做到对关键源结点的路由路径隔离，RAC 需要毒化规避的自治系统数目实际在数千个；理论的 BGP 协议中可以

附带约 2000 个结点的毒化，但是实际上限于路由器厂商技术建议、路由器系统实现以及 ISP 服务商的安全限制，实际的 BGP 路由更新仅允许附带 255 个结点的毒化；

- 如果弱化对关键源结点路由路径的绝对隔离要求，允许存在一定的路径泄漏，基于作者实现的一组贪心策略，通过实验可以发现在仅允许 255 个毒化约束下，RAC 并不能够为关键数据流提供一个很好的洪泛攻击防御。

后续作者还设计了一个针对 RAC 重路由洪泛攻击防御策略的攻击模型，通过模拟实验验证了路径泄漏的易发觉性、路由毒化后导致后续网络收敛困难、实际 255 个结点毒化约束下可行候选路由旁路过少等问题。

总的来说，本文的一个最大的突出点在于作者对于实际技术进行分析时，没有局限于基本的理论情形，而是将技术放到了实际的运用场景之中进行分析，具备了更强的现实价值。另外文章通过对现实中技术问题的挖掘，可以分析得到理论协议到实际应用的瓶颈所在，在这里是 ISP 服务商的限制和路由器制造厂商的简化实现。另一点是文章突出强调了新的安全技术、网络协议在设计之中需要一个真实的评估场景，这样才能得到一个更加实际有效的技术方案。

纵观全文，个人觉得文章还是存在着一定可以改进的地方。在论证关于弱化对关键源结点路由路径的绝对隔离要求部分时，作者使用了自己设计的一套贪心策略来执行毒化结点的选择，并基于上述算法进行了后续的一系列实验评估，试图说明即便弱化绝对路径隔离这一要求也很难为关键数据流形成一个良好的洪泛攻击防御。虽然这样的贪心近似算法直观上是合理的，且文章阐述了该问题的最优解是一个 NP 完全问题，但是这让读者很难相信是否存在另一个同样合理的策略使得得到的解是一个能够有效抵御洪泛的情况。个人觉得如果可以加上更加严谨的数学论证，找到 NP 问题近似算法的一个最坏近似比，这样使得后续的说明论证能够更加有力。