一种基于 MIPv6 的移动目标防御反审查方法

张 舒 婷
(太原学院计算机工程系 山西 太原 030032)

摘 要 虽然互联网已经成为生活中各个方面的中心,但仍有很多用户无法通过互联网自由地获取信息。攻击者可以通过部署审查者实现对用户特定信息的屏蔽。从网络信息提供者的角度出发,提出一种面向用户的反审查方法,使攻击者的攻击代价大大增加。通过使用移动 IPv6 来形成移动目标防御策略,使 Web 服务器从逻辑上表现为移动节点(实际上没有移动)。对该方案进行建模(概率模型)分析,提出一个关键参数—分群比,将攻击者所需资源与实际条件限制进行对比。在该模型的基础上搭建现实原型(对服务器软件和内核进行简单修改而不改变标准移动 IPv6 协议),以此证明可以在不改变现有网络基础设施的情况下使用该方法。通过实验分析该方法性能开销。

关键词 反审查制度 移动目标防御 移动 IPv6

中图分类号 TP311 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2019.04.052

A MOVING TARGET DEFENSE ANTI-CENSORSHIP METHOD BASED ON MIPV6

Zhang Shuting
(*Department of Computer Engineering, Taiyuan University, Taiyuan 030032, Shanxi, China*)

Abstract Although the Internet has become the center of all aspects of our lives, there are still many users cannot freely access to information through the Internet. Attackers can shield users' specific information by deploying censors. From the perspective of network information providers, we proposed a user-oriented anti-censorship method to greatly increase the cost of attackers. By using mobile IPv6 to form a mobile target defense strategy, Web servers were logically represented as mobile nodes (virtually no movement). The scheme was modeled (probability model) and analyzed. A key parameter, the swarm ratio, was proposed to compare the attacker's resource requirements with the actual constraints. On the basis of this model, a real prototype was built (simple modification of server software and kernel without changing the standard mobile IPv6 protocol) to prove that the scheme could be used without changing the existing network infrastructure. Performance overhead was measured by experiments.

Keywords Anti-censorship Moving target defense Mobile IPv6

0 引 言

近十年来,互联网的广泛使用给人们生活方式带来重大改变。通过计算机或移动终端可以很容易地获得信息的能力促进科学技术和文化传播的快速发展。虽然有些人认为这是互联网的弊端,它使全世界的团体机构比以往任何时候都更加紧密。但是,对大多数人而言,自由获取信息是他们生活不可或缺的一部分,甚至能够帮助他们在科学、技术、数字文化等各个领域发挥潜力。

但是某些别有目的的攻击者总是试图阻止人们访问某些类型的信息。当前有多种方法可以阻止查看网络信息,常见的技术包括[1]:(1) IP 地址阻塞:对由 IP 地址标识的某些站点进行阻塞访问;(2) 域名系统(DNS)过滤:阻止访问某些未被解析的域名;(3) 统一资源定位符(URL)过滤;(4) 数据包过滤。

大多数用户利用加密隧道和代理来绕过这些审查

收稿日期:2018 - 09 - 24。**张舒婷**,讲师,主研领域:网络安全。

方法,如 VPN[2-4]和 Tor[5]。作为响应,攻击者通常试图查找和阻塞提供服务的主机。

本文提出了一种结合移动 IPv6(MIPv6)和移动目标防御(MTD)技术特点的解决方案。基于 MTD 思想,通过检测洪泛攻击来防止分布式拒绝服务(DDoS)攻击,使服务器变成移动目标[6-8]。该方法也可用来保护用户隐私[9]。它与现有的反审查措施不同,用户不必直接对抗审查措施。并且该方法与现有的反审查方法可以共存。

在 MIPv6 中,通常使用永久 IP 地址(归属地址)来避免 TCP 会话的中断,使用一个或多个转交地址 CoA(Care-of Address)来连接其他节点[10]。应用 MIPv6 将 Web 服务器视为移动节点,利用动态改变的 IP 地址(基于 CoA)避免过滤和阻塞等攻击行为。将端用户随机分组,并提供一个可以用来访问网站的 CoA。一段时间之后,对用户重新分组,并用新生成的一组 CoA 更新用户。本文所提方案的基本架构如图 1 所示,在服务器端,n 个不同的 CoA 被随机分配给不同的用户组。一段时间后,用户重新分组,并将通过新生成的 CoA 与服务器连接。MIPv6 的有效性取决于所使用 CoA 的数量和伪装成正常用户的攻击者数量,攻击者通过查找 CoA 来实施阻塞,通过改变 CoA 将用户变为移动目标。本文提出一种新的地址变化方法,大大增加了攻击者查找地址的代价。该方法利用了现有的 MIPv6 技术,因此不需改变现有的 MIPv6 协议。

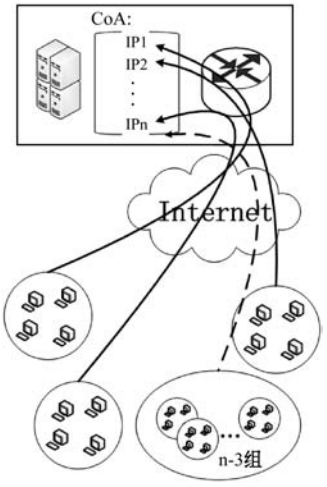


图 1　基于 MIPv6 的基本架构

1　相关研究

1.1　反审查技术

用户利用代理和加密隧道技术绕过审查,如 VPN[2-4]和开源的 HTTPS 代理。然而攻击者可以通过阻塞提供服务的系统 IP 地址来阻止这些方法。

近年来,一种叫作“路由诱骗”的技术被提出[11]。传统方法中的代理部署在网络路径的末端,而该方法把代理部署在网络的中间[12-14]。其中的互联网服务提供方 ISP(Internet service providers)过滤被标记信息(发送至虚假地址),然后将其重新发送至真实目的地址(被审查地址)。过滤过程需要耗费计算资源和额外的硬件资源,并且为用户带来延迟。当前的路由诱骗技术依然无法有效防御流量分析和网站指纹识别方法。

1.2　移动目标防御技术

文献[7]提出一种基于云平台的防御网络 DDoS 攻击机制。它首先对服务器进行选择复制,对客户端进行重新分配,使被攻击的服务器变成移动目标。被攻击的服务器被部署在其他网络中的复制品代替,客户端也被移植到该新的服务器上。客户端迁移之后回收被攻击的服务器进行循环利用。只有迁移到服务器的客户端才知道其新地址,新加入的客户端通过 DNS 服务将其引导至服务器受保护的云平台。

该方法运用至反审查策略中的限制条件如下:(1) 审查者能发起 IP 阻塞和 DNS 过滤来阻止用户访问服务器;(2) 普通客户端群组中检测审查者比较困难,与该审查者在同一分组的用户将被永远阻塞;(3) DDoS 需要向目标服务器发起大流量攻击,一旦检测到服务器的正确地址,单个审查者就能完成攻击,这将导致服务器的频繁变换;(4) 服务器重定向过程会导致丢包;(5) 复制大量的服务器资源需要建设相应的大规模云平台。

文献[9]提出一种 MT6D 方法,它是一种动态的、网络层的 MTD,在不中断和不重新发起会话的前提下,快速改变处于会话中的发送方和接收方的 IPv6 地址。MT6D 利用了 IPv6 的优势,创建动态的接口识别 IID(Interface Identifier)来生成动态的 IP 地址。这些 IID 由以下几部分组成:(1) 每个主机需要一个独特值作为种子 IID;(2) 收发双方共享密钥;(3) 参数改变需要收发双方的同意。

MT6D 通过带外分享种子 IID 和共享密钥,对每个数据包按照 UDP 协议封装并利用虚拟 IP 地址隐藏真实的 IP 地址。然而该方法仅支持点对点网络,普通的客户端-服务器网络没有考虑在内[15]。MT6D 的限制条件如下:(1) 由于地址冲突造成数据包丢失;(2) 时间必须严格同步;(3) 一个虚拟 IP 对应一个用户这种方式可扩展性不够;一个虚拟 IP 对应一个用户组,这

种方式如果组里有一个审查者,该用户组可以被永久阻塞。

2 背景介绍

2.1 移动 IPv6 的使用

MIPv6 最重要的特点[16]是:一个 IP 地址可变的移动节点 MN(Mobile Node)在网络中移动时依然能够接收到消息。假设服务器是一个移动节点,在 MIPv6 中,MN 有一个永久的 IP 地址,称为归属地址 HoA(Home Address),由归属代理 HA(Home Agent)分配。归属代理是 MN 归属链路上的路由器,其功能类似于 MN 的代理。MN 也有一个备用地址,称为转交地址 CoA(Care-of Address),由通信对端节点 CN(Correspondent Nodes)使用与 MN 保持通信。HA 保持与 CoA 的联系,并执行必要的转发。MN 通过包含新 CoA 的绑定更新 BU(Binding Update)消息更新 HA,HA 发回绑定确认 BA(Binding Acknowledgement)消息作为响应。CN 通过 HoA(由 HA 生产并由隧道传送到 MN)与 MN 建立通信。

2.2 路由优化

路由优化过程实现了 MN 和 CN 之间的数据包传输路径最短。CN 需要知道 MN 当前绑定信息。因此,MN 必须通过 CoA 更新 CN。路由返回过程用于验证所请求的 CoA[17]和 HoA 的使用权限。此过程涉及四个消息,路由优化还使用两种额外消息(BU 和 BA)。当只需要 CoA 测试消息时这些开销便会减少[18]。

文献[19]中指出与路由返回测试相关的所有消息都通过使用共享对称密钥来消除。首先,路由优化的低信令开销将切换延迟最小化,这反过来又减少了在地址变化期间的丢包。其次,在不需要路由返回的情况下,HA 可不参与路由优化。MN 可以直接用新的 CoA 更新 CN,从而与 HA 断开连接。尽管如此,静态共享密钥方法也有一些局限性:(1) CN 需要信任 MN 的行为,并且需要假设 MN 不会对第三方发起洪泛攻击[20]。(2) MN 和每个 CN 之间的共享对称密钥可能导致重放攻击。使用 IPSec 与 MN 和 CN 之间的互联网密钥交换 IKE(Internet Key Exchange)可解决这一问题。

在运行路由优化机制之后,数据包将通过 CN 直接路由到 MN 的 CoA。为了将数据发送到任何一个 IPv6 的目的地址,使用第二类路由和目的地址选项头将数据包传送至 MN[21]。

第二类路由头是一种支持 MIPv6 的路由报头类型。当数据包被发送到 MN 的 CoA 时,HA 或 CN 使用该路由头携带 MN 的 HoA。例如,如果 CN 知道 MN 的 CoA,则 CN 可以向 CoA 发送数据,但是 MN 需要从目的地址中获取其 HoA 信息。因此,CN 在第二类路由头中存储 MN 的 HoA,然后以 MN 的 CoA 作为目的地址发送数据。当 MN 接收到数据时,它自动将数据的目的地址替换为存储在第二类路由报头中的地址。

目的地选项头用于承载仅需要由目的节点处理的可选信息,其中很重要一点就是归属地址。当 MN 不在归属地时,它发送的数据中就含有该选项信息(将其 HoA 发送给 CN)。此时,数据包的源地址是 MN 的 CoA,而归属地址选项中的地址是 MN 的 HoA。当地址的有效性被验证之后,这两个地址将被交换。MN 的 CoA 和 HoA 必须在注册时相互绑定。

2.3 多转交地址

移动目标防御用于反审查的关键技术之一是多 IP 地址能力,使得审查者不能在有限的时间内检测到地址并实行阻塞。随着 MIPv6 和绑定识别 BID(Binding Identification)号码的扩展,MN 可以实现多个 CoA 绑定同一个 HoA。MN 可以设置多个 IPv6 全局地址并将其注册为它的 CoA。为了注册多个绑定,MN 为每个 CoA 生成一个独特的 BID。这些 BID 被存储在绑定更新列表中,且每条绑定信息都是相互独立的。MN 可以通过 BID 移动性选项使用 BU 消息注册其 CoA。

另一方面,可以在 CN 上禁用多转交地址。这样 CN 就无法识别接收到的 BU 消息中 BID 移动性选项。根据 RFC 5648[22]协议,CN 可以跳过未知的移动性选项,仅简单地更新绑定缓存,并将数据包发送到 MN 最新更新的 CoA。

3 基于 MIPv6 的 MTD 反审查方法

本节描述了基于 MIPv6 的移动目标防御 MI-MTD(MIPv6-based Moving Target Defense)方法,并通过建模来协助分析影响方案有效性的各种因素。最后,通过实验结果证明所提方案的可行性。

该方法的核心技术就是使用多个 IPv6 的 CoA。与实际的移动应用不同,主机(如:Web 服务器)被视为移动节点,HoA 作为服务器的永久地址,CoA 作为动态地址。被分配 CoA 的用户组称为访问组。每隔一段时间生成伪随机 IP 地址,替换服务器的所有 CoA。在每个间隔内,通过地址变化和重新分配用户,随机改

变每个访问组成员身份。通过绑定更新机制用新的 CoA 更新用户。

本文所提出的方案只需要在服务器中设置 MIPv6 参数,为 HoA 选择一个与服务器子网前缀不一样的 IP 地址。当 MIPv6 运行时,服务器从其路由器接收路由宣告消息,该路由器归属链路的前缀与 HoA 的前缀不同。这样,服务器就认为它在外地网络中,并在本网络中注册一个 CoA。随机生成 64 位地址,与归属链路前缀结合来生成新的 CoA。这些新的 CoA 在子网中注册之前通过邻居请求消息来检测是否已经被占用。根据 MIPv6 的多个 CoA 注册规则,服务器(MN)将会向其用户发送含有新 CoA 的 BU 消息。当用户接收到 BU 时,服务器的 HoA 和 CoA 被插入到绑定缓存中,并删除以前的 CoA。

为了部署 MIPv6,服务器端需要一些改变:(1)允许对不同访问组进行用户分配;(2)通过分配的 CoA 更新每个访问组。用户端不需要任何改变,MIPv6 协议标准也不需改变。

该方法的两个关键之处在于多个 CoA 的分配和变化。将不同的 CoA 分配给每个访问组限制了一个组内有一个审查员(假装成正常用户的攻击者)的影响。一旦审查者发现一个 CoA,它将阻塞该地址来切断对可能通过 CoA 产生的服务器访问。所有与此审查者在同一访问组中的用户都将失去与服务器的连接。为了解决这个问题,每隔一段时间使用户地址在不同访问组之间随机变化。为了消除地址变化期间的丢包,在删除以前的 CoA 之前,服务器要为新的 CoA 发送 BU 消息。因此,在切换延迟期间,用户发送的数据报头中含有旧的 CoA。每个访问组中的所有用户接收到各自的 BA 或在一段时间之后,服务器删除旧的 CoA。地址变化间隔可以动态变化,为方便分析,本文使用了固定变化间隔。

3.1　模型与分析

本文通过分析攻击者伪装成正常用户所付出的代价来衡量 MI-MTD 方案的有效性。审查者在每个变化间隔之后都会接收到含有最新 CoA 的 BU 消息,该 CoA 将被阻塞或攻击。在每个间隔期间,包含至少一个审查者的访问组中的所有端用户将被禁止访问服务器。首先计算在任意时刻,用户被阻塞的概率与 CoA 和审查者的数量的关系。

建立变化过程的数学模型来协助分析。该模型中使用的符号如表 1 所示。

表 1　模型使用符号对应表

N	用户总数
N_a	攻击者的代理数量
N_u	未被攻击的用户数量
I	每个时间间隔内所使用的 IP 地址(CoA)数量
A_j	IP_j分配给的用户,$j=1,2,\cdots,I$
P_j	IP_j没有被阻塞的概率
N_{ub}	与审查者在同一组的用户数量
N_{uf}	没有与审查者在同一组的用户数量
p	访问概率
b_k	k 个变化间隔之后的阻塞概率
t	变化间隔大小
ϕ	分群比

用户总数 N 是审查者(N_a)和正常用户(N_u)的和。在每个变化间隔中,正常用户可分为两类:被审查者和未被审查者。访问概率 p 是用户在任意时刻访问服务器的概率。为了计算 p,首先需要计算未被审查者数量(N_{uf})的期望值:

$$N_{uf} = \sum_{j=1}^{I} P_j A_j \tag{1}$$

假设访问组大小与式(1)相同,则用户在可用 CoA 上均匀分布,即 N 可以被 I 整除。

$$A_j = \frac{N}{I} \tag{2}$$

因此,对于任意 CoA,IP_j未被阻塞的概率为:

$$P_j = \frac{\binom{N-N_a}{A_j}}{\binom{N}{A_j}} \tag{3}$$

式中:$\binom{N-N_a}{A_j}$是审查者没有在 A_j组中方式的数量,$\binom{N}{A_j}$是从 N 个用户中选择 A_j用户方式的数量。因此:

$$E[N_{uf}] = \sum_{j=1}^{I} A_j \frac{\binom{N-N_a}{A_j}}{\binom{N}{A_j}} \tag{4}$$

基于上述假设,$A_j = A_i, \forall i,j \in (i,j), N = I \times A_j$,由此可得:

$$E[N_{uf}] = N \times \frac{\binom{N-N_a}{A_j}}{\binom{N}{A_j}} \tag{5}$$

基于斯特林公式 $n! \approx \left(\frac{n}{e}\right)\sqrt{2\pi n}$，假设 $N_a << N$，则：

$$E[N_{uf}] = N \times \left(\frac{N - N_a}{N}\right)^{A_j} = N\left(1 - \frac{N_a}{N}\right)^{N/I} \quad (6)$$

因此，用户在给定时刻访问服务器的概率 p 为：

$$p = \frac{N}{N_a}\left(1 - \frac{N_a}{N}\right)^{N/I} \quad (7)$$

例如，假设有 1 000 000 个用户和 5 000 个审查者，在每个变化间隔中使用 10 000 个 CoA，对于任意用户，在一个变化间隔期间访问服务器的概率大约为 60.88%。

基于上述结果来考虑实际（如网站访问模式）中的其他重要因素。比如：用户访问网站上的特定信息通常不与 Web 服务器以连续的方式进行交互。也就是说用户并不是一直点击和加载网页。典型的访问模式是用户先与服务器短暂交互，然后浏览自己机器上已经呈现的信息（持续时间较长）。基于本文提出的变化机制所求得的访问概率是相互独立的，由此可较容易计算出在一段时间 δ 内的阻塞概率 b_k，其中 k 表示变化间隔的数量，则 k 个独立时间间隔内，受审查的用户被阻塞的概率为：

$$b_k = (1-p)^k \quad k = \left[\frac{\delta}{t}\right] \quad (8)$$

以 1 分钟为例计算该期间的阻塞概率，设定变化间隔 t 为 10 s，则 $b_6 = (1 - 0.608\ 8)^6 \approx 0.358\%$。即用户每分钟大概有 99.6% 的几率可以成功访问服务器。

本文所提方案的整体效果取决于参数之间的关系。首先，定义关键参数分群比 $\phi = \left(\frac{N_a}{I}\right)$，它决定了访问和阻塞概率并且不受网络规模的影响。也就是说，只要分群比保持不变，改变 N_a 和 I 的值不会影响访问概率，改变 N_u 也不会对其产生影响。显然，如果 N 小于 I，用户可以成功访问服务器。随着 N 的增加，访问概率逐渐收敛。例如，在上一个例子中 $\phi = 0.5$，访问概率 p 大于等于 60.65%。当用户数足够多时，可以计算访问概率的最小值，它是分群比的函数。

通过计算分群比的最大值可以得出系统可用的最低概率 p，这与具体的应用场景有关。例如，在极限条件下，每几小时可以访问服务器一次已经足够满足用户需求。相比之下，典型的通过网页浏览新闻可能每隔几分钟左右就需要访问服务器一次。因此，衡量有效性与攻击者的攻击方式（完全阻塞或仅制造一点不便）有关。为方便说明，本文以一分钟制造 5% 的阻塞为例，如果用户在一分钟内访问网站的概率达不到 95%，则认为系统被破坏，而实际上这仅给用户造成些许不便。用户在审查者干预下将要承受更高的阻塞率。

在本例中，当 $\phi = 0.933\ 9$ 时达到最大值，因此可以讨论 IPv6 地址空间和网站硬件资源限制问题。Web 服务器在一个子网中能够利用的 IP 地址数量为 2^{64}，服务器在一个变化间隔内可以利用的 CoA 数量取决于两点：（1）如果 2^{64} 个地址全部使用，服务器在一个间隔内全部用完，访问组将无法收到新的 CoA。当然，对于服务器系统来说同时使用 2^{64} 个地址就目前的技术水平来说不太现实。如果每个间隔使用 1 000 000 个 CoA，5.849×10^7 年之后才会用光这些地址。（2）每个间隔用于创建和绑定 CoA 的 IP 地址受服务器和路由的硬件条件限制。由文献[15]可知，取 I 值为 10 000（不会带来较大延迟），为了使分群比 $\phi = 0.933\ 9$，$N_a = 0.933\ 9 \times 10\ 000 = 9\ 339$，即攻击者必须每分钟利用 9 339 个审查者才能导致大于 5% 的阻塞率。以此类推，如果攻击者想要达到持续 10 小时（足够阻止用户下载一条新闻信息）造成 99% 以上的阻塞率，分群比 $\phi = 0.12$，需要部署 12 800 个审查者。以 5 分钟注册为例，攻击者需要1 067人才能在第 10 个小时完全阻塞注册过程，这意味着 10 小时之内用户依然可以访问网站。为了实现完全阻塞 10 小时，攻击者需要在一开始就部署 128 000 个审查者。当服务器重置用户时需要重复执行这些过程。图 2 展示了三种不同时间内，攻击者为了达到不同等级的阻塞所需的分群比。可以看出，阻塞时间越长，阻塞率越高，所需的分群比越高，即需要在网络中部署的审查者越多。

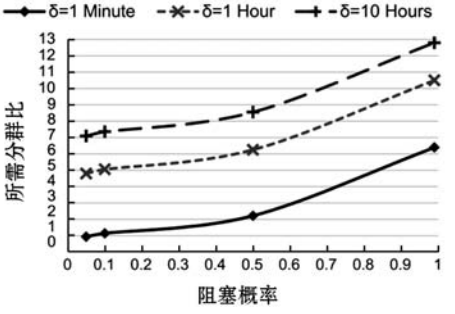


图 2 不同阻塞概率所需的分群比大小

3.2 用户注册过程

实际上，攻击者不需要 N_a 台电脑来模拟 N_a 个审查者。攻击者可以创建一个绑定多个 IP 地址的系统。由文献[15]可知，55 000 个 IPv6 地址可以同时绑定在同一台机器（Intel i7 处理器，3.4 GHz，16 GB RAM，千兆以太网接口）上，即攻击者可以部署 55 000 个审查者。为了防御审查者，需要人为干预，对用户来说，只需要在初始注册的时候操作一下即可。一些其他方法，比如复杂的验证码检验，需要用户花费大量时间来

处理。

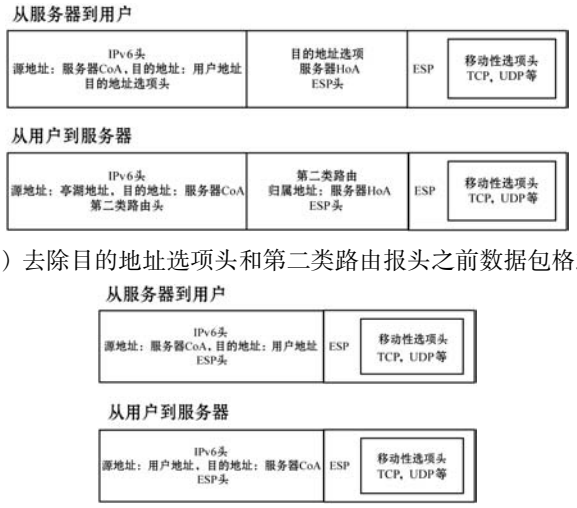
注册状态应该每隔一段时间(如 12 小时)重置一次,迫使攻击者的每一个审查者都要重复注册过程。另一个重要因素就是每一个审查者的使用时间。如果审查者在每一次注册开始时立即部署,则它在整个变化期间都会有影响。如果审查者在第 11 个小时部署,那他仅在下 1 个小时内有效,之后便重新注册。如上所述,12 小时的注册周期,10 小时内造成完全阻塞,1 分钟的解决时间,攻击者需要在注册重置前 2 个小时内准备 128 000 个审查者。这样在接下来的 10 个小时内,没有用户能够访问服务器。在这种情况下,攻击者需要 1 067 人操作 2 个小时。在服务器端,可以相对容易地额外增加计算机附件、网络接口和路由器。为了攻击配有 10 个服务器(配有 10 个接口)的站点,攻击者需要 106 700 个并行工作的人。此外,在第 1 个小时内,仍有大量用户能够访问服务器。

由于本方案中不存在 HA,新用户将无法使用服务器的 HoA 连接到服务器。相反,服务器在接收到用户的请求时,由它发起连接。在用户端,需要使用服务器的 HoA 和域名来设置主机文件。新用户为了连接服务器,必须向服务器发送其 IP 地址和共享密钥。一个简单的方法是利用安全邮件来完成交换。

3.3　IPsec

当节点 N1 向另一个节点 N2 发送数据包时,需要在数据包报头中添加源地址(作为 HoA)和目的地址。然后,N1 检查绑定更新列表是否已经将 BU 发送到 N2,从 N2 处搜索 CoA。如果发现,N1 将其 CoA 写进归属地址选项中,检查其绑定缓存以确定 N2 的 BU 是否已送达。如果发现,N1 将生成包含 N2 的 CoA 的第二类路由报头。含有源地址和目的地址的数据包将送达 IPSec。加密后添加报头,归属地址选项与源地址交换,第二类路由报头与数据包目的地址交换。当 N2 收到数据包时,按照报头在数据包中出现的顺序进行处理。IPSec 过程 HoA 总是在数据包报头中的源地址和目的地址中[23]。IPSec 没有加密第二类路由报头和归属地址选项。

为了防止审查,可以删除数据包中目的地选项头(和第二类路由报头)来解决这个问题。在 IP 封装安全有效载荷 ESP(Encapsulated Security Payload)报头中的安全参数索引 SPI(Security Parameter Index)足以访问 HoA(数据包的真实源地址和目的地址)。删除目的地选项头和第二类路由报头之前和之后的数据包格式如图 3 所示。



(a) 去除目的地址选项头和第二类路由报头之前数据包格式

(b) 去除目的地址选项头和第二类路由报头之后数据包格式

图 3　去除目的地选项头和第二类路由报头之前和之后的数据包格式

3.4　原型实现

为了证明本方案的有效性,并对该设计的性能进行评估,搭建一个基于 IPv6 的测试台如图 4 所示。使用三台路由器(R1、R2、R3)和五台 Ubuntu 14.04 系统(Linux 内核版本 3.8 - 2)的计算机(2.4 GHz 双核 CPU,4 GB DDR2,800 MHz RAM)。基于 Linux 的开源 MIPv6(UMIP),路由器 R1 作为因特网的“中心”。审查者之间像路由器一样转发数据,单个访问组的用户(USER1、USER 2 和 USER 3)使用一个 CoA,审查者不在该组中。

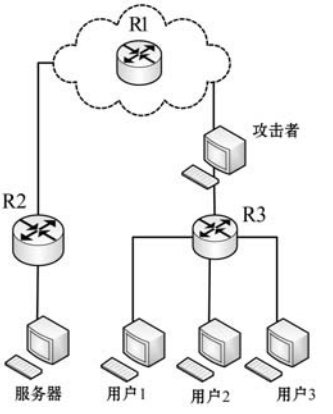


图 4　测试台的网络拓扑图

开启服务器和用户的可移动进程,服务器的 HoA 与 R2 的路由宣告不在同一个网段。服务器在 R2 上的注册地址为 CoA 并将其更新到所有用户。通过编程来实现每 10 秒生成一个新的 CoA(实时删除前一个)。根据 MIPv6,服务器向用户发送 BU 消息告知其新的 CoA。BU 消息的 ACK 比特使用户发回 BU 的确认响应消息,以保证用户成功接收 BU 消息并更新其绑定缓存条目。因此,每 10 秒便在服务器和每个用户之间产生两个开销数据包,如图 5 所示。图中,实线表

示服务器端,源地址为服务器 CoA,目的地址为用户地址,目的地址选项头中的归属地址为服务器 HoA;虚线表示用户端,源地址为用户地址,目的地址为服务器 CoA,第二类路由头中的归属地址为服务器 HoA。通常,在此更新期间,用户在接收到 BU 消息之前无法访问服务器。在服务器端注册多个 CoA 可以解决这一问题,也就是说直到用户接收到下一个 CoA 之前,当前时间间隔内的 CoA 保持有效。一旦所有用户更新到新的 CoA 才删除当前 CoA。

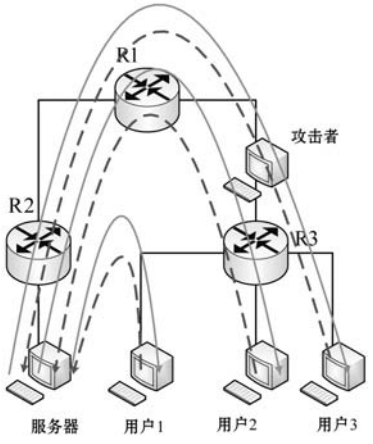


图 5 绑定更新过程

本文方法会产生两种开销,更新过程 BU 和 BA 消息产生的信令开销和服务器和用户之间传输数据产生的传输开销。

信令开销:一个完整的节点注册过程需要与服务器传输两类消息(BU 和 BA 消息),每条消息 110 字节(使用 IPSec,移除目的地址选项和第二类路由报头)。在最初的 MIPv6 中,BU 和 BA 的长度是 110 字节,由于使用路由返回机制,会有四条额外信息。此外,为了最小化消息数量,减少开销,该系统可以不使用 BA 运行,即如果数据从客户端传输新的 CoA,服务器知道客户端接收到 BU 就不需要 BA 消息。

传输开销:在应用 IPSec 条件下,每个数据包会产生 24 字节的开销。即便不使用本方法,仍然需要使用 IPSec 来确保服务器和用户之间建立安全连接,所以本文方法对每个数据包造成的实际开销包为零。

4 结 语

本文基于移动 IPv6 和移动目标防御技术提出一种反审查机制架构。并通过理论分析证明,通过改变分群比率值,可以使攻击者部署审查机制的代价大大增加。该方法不改变标准 MIPv6 和网络协议,也不需要第三方中介介入。最后通过设计一种基于 MIPv6 的测试实验平台证实该方案的可行性。

参 考 文 献

[1] 刘麒, 徐阳, 吕婷,等. 基于 HTML5 WebWorker 组件的 DDoS 攻击方式和检测[J]. 计算机应用与软件, 2016, 33(12):295 - 300.

[2] F-Secure Switch on Freedom[OL]. 2015 - 04 - 10. http://f-secure. se. whoisbucket. com/.

[3] Free VPN Service Free VPN Software—Hotspot Shield VPN [OL]. 2015 - 04 - 10. http://www. hotspotshield. com/.

[4] Psiphon Uncensored Internet Access For Windows and Mobile[OL]. 2015 - 04 - 10. https://psiphon3. com/en/index. html.

[5] Degabriele J P, Stam M. Untagging Tor: A Formal Treatment of Onion Encryption[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Cham, 2018:259 - 293.

[6] Sengupta S, Vadlamudi S G, Kambhampati S, et al. A Game Theoretic Approach to Strategy Generation for Moving Target Defense in Web Applications[C]//Conference on Autonomous Agents and Multiagent Systems. International Foundation for Autonomous Agents and Multiagent Systems, 2017:178 - 186.

[7] Wang H, Jia Q, Fleck D, et al. A moving target DDoS defense mechanism[J]. Computer Communications, 2014, 46:10 - 21.

[8] Venkatesan S, Albanese M, Amin K, et al. A moving target defense approach to mitigate DDoS attacks against proxy-based architectures[C]//Communications and Network Security. IEEE, 2017:198 - 206.

[9] Dunlop M, Groat S, Urbanski W, et al. MT6D: A Moving Target IPv6 Defense[C]//Military Communications Conference. IEEE, 2012: 1321 - 1326.

[10] Meng R, Da B, Wang C. IP mobility enhancements for MIPv6 and PMIPv6[C]//Tenth International Conference on Mobile Computing and Ubiquitous Network. IEEE Computer Society, 2017:1 - 6.

[11] Karlin J. Decoy Routing: Toward Unblockable Internet Communication[C]//Proceedings of the USENIX Workshop on Free and Open Communications on the Internet (FOCI'11), 2011.

[12] Houmansadr A, Nguyen G T K, Caesar M, et al. Cirripede: Circumvention Infrastructure using Router Redirection with Plausible Deniability[C]//Proceedings of the 18th ACM conference on Computer and communications security. New York: ACM, 2011:187 - 200.

[13] Wustrow E, Swanson C M, Halderman J A. TapDance: end-to-middle anticensorship without flow blocking[C]//Proceedings of the 23rd USENIX conference on Security Symposium. USENIX Association, 2014: 159 - 174.

[14] Wustrow E, Wolchok S, Goldberg I, et al. Telex: Anticen-

sorship in the network infrastructure[C]//Proceedings of the 20th USENIX conference on Security. USENIX Association Berkeley, 2011.

[15] Morrell C, Ransbottom J S, Marchany R, et al. Scaling IPv6 address bindings in support of a moving target defense [C]//The 9th International Conference for Internet Technology and Secured Transactions(ICITST-2014). IEEE, 2015: 440 - 445.

[16] 郭志强, 王振兴, 张连成,等. 基于 Hash 生成地址的移动 IPv6 高效安全路由优化方案[J]. 计算机应用与软件, 2016,33(6):105 - 109.

[17] Heydari V, Kim S I, Yoo S M. Anti-Censorship Framework using Mobile IPv6 based Moving Target Defense[C]//Proceedings of the 11th Annual Cyber and Information Security Research Conference. ACM, 2016.

[18] Arkko J, Vogt C, Haddad W. Enhanced Route Optimization for Mobile IPv6[EB/OL]. RFC 4866, Internet Requests for Comments,May 2007.

[19] Perkins C. Securing Mobile IPv6 Route Optimization Using a Static Shared Key[EB/OL]. RFC 4449, Internet Requests for Comments,Jun. 2006.

[20] Nikander P, Arkko J, Aura T, et al. Mobile IP Version 6 Route Optimization Security Design Background[EB/OL]. RFC 4225, Internet Requests for Comments, Dec. 2005.

[21] Kang D, Jung J, Lee D, et al. Security analysis and enhanced user authentication in proxy mobile IPv6 networks [J]. Plos One, 2017, 12(7):e0181031.

[22] Wakikawa R, Devarapalli V, Tsirtsis G, et al. Multiple Care-Of Addresses Registration[EB/OL]. RFC 5648, Internet Requests for Comments, Oct. 2009.

[23] Guo N, Peng F, Gao T. Secure Mobility Management for MIPv6 with Identity-Based Cryptography[M]//Information and Communication Technology. Springer International Publishing, 2015.

(上接第 325 页)

本文改进方案的验证方程为 $y^s n^r r^n \bmod p = g^m m^{r+n} \bmod p$,由于 m 同时出现在指数和底数中,即使验证方程中的其他参数均已知,也无法求出 m 的值,故第 4 节中的四种攻击方法均无法攻击成功,改进方案安全。

(5) 防止参数 k 同态攻击:假设签名者使用相同的参数 t 和不同的 k_1、k_2、k_3 对消息 m_1、m_2、m_3 签名,满足 $k_3 = k_1 + k_2 \bmod p - 1$,签名分别为:$(m_1; r_1, s_1, n_1)$、$(m_2; r_2, s_2, n_2)$、$(m_3; r_3, s_3, n_3)$,则有:

$$s_1 = (m_1 - tr_1 - k_1 n_1) x^{-1} \bmod p - 1$$

$$s_2 = (m_2 - tr_2 - k_2 n_2) x^{-1} \bmod p - 1$$

$$s_3 = (m_3 - tr_3 - k_3 n_3) x^{-1} \bmod p - 1 = (m_3 - tr_3 - (k_1 + k_2) n_3) x^{-1} \bmod p - 1$$

其中:x、t、k_1、k_2 未知,3 个方程 4 个未知量,无法求解,故同态攻击无法成功。

6 结　语

本文对各类改进的 ElGamal 离散对数数字签名方案进行了分析,对改进方案李丽娟方案进行了攻击分析,给出了 4 种攻击方法,证明了其存在安全缺陷。给出了一个新的改进方案,证明了其正确性和安全性,证明了其可防止伪造签名攻击和同态攻击。很好地解决了无 Hash 函数的 ElGamal 数字签名的改进问题。

参 考 文 献

[1] Diffie W, Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644 - 654.

[2] El-Gamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Trans. Inf. Theory, 1985, 31(4):469 - 472.

[3] Wang X, Lai X, Feng D, et al. Cryptanalysis of the hash functions MD4 and RIPEMD[C]//Proceedings of the 24th annual international conference on Theory and Applications of Cryptographic Techniques. Berlin:Springer-Verlag,2005.

[4] Wang X Y, Yu H B. How to Break MD5 and other Hash Functions [C]//Eurocrypt 2005. Berlin: Springer-Verlag, 2005: 1 - 8.

[5] Wang X Y, Yin Y L, Yu H B. Finding Collisions in the Full SHA-1[C]//Proceedings of the 25th annual international conference on Advances in Cryptology. Berlin:Springer-Verlag,2005: 17 - 36.

[6] 曲娜, 杜洪军, 颜达, 等. ELGamal 数字签名算法的一种变形[J]. 吉林大学学报(信息科学版), 2009, 27(6): 590 - 594.

[7] 张会影, 张军. 一种改进的 ElGamal 数字签名方案的研究与设计[J]. 计算机工程与科学, 2009, 31(12):35 - 37.

[8] 周克元. 对两个离散对数数字签名算法的攻击与改进[J]. 科学技术与工程, 2013, 13(32):9725 - 9729.

[9] 白荷芳, 王彩芬. 对一种变形 ELGamal 签名体制的分析[J]. 西北师范大学学报(自然科学版), 2006, 42(3): 109 - 110.

[10] 芦殿军,张秉儒. EIGamal 签名方案的安全性分析与改进[J]. 长江大学学报(自然科学版),2008,5(1):193 - 194.

[11] 李晓峰, 赵海, 王家亮, 等. 基于增加一个随机数的 ElGamal 数字签名算法的改进[J]. 东北大学学报(自然科学版), 2010, 31(8):1102 - 1105.

[12] 李丽娟,郭亚杰. 一种改进的 ElGamal 数字签名方案[J]. 计算机工程与科学,2016,38(6):1097 - 1102.