能源企业防御 DoS 攻击的端信息跳变技术研究

司凯文　李世尧（晋能控股装备制造集团科技信息部，山西　晋城　048000）

摘　要：对于能源企业来说，DoS 攻击是当前网络攻击中影响最大、危害最深的攻击之一，基于静态性、相似性、确定性构建的信息系统已难以应对现在的高强度 DoS 攻击。本文研究的端信息跳变技术是形成易守难攻防御能力的很好途径，在端到端数据传输中，通信二者或一方根据端口、地址、时隙、加密算法或协议随机改变端到端信息。破除网络各要素的静态性、相似性、确定性，从而破坏敌方攻击与干扰，实现主动网络防御。我们在部署 web 服务器过程中，将端信息跳变技术引入 web 插件，实现了在 web 访问中主动防御 DoS 攻击的功能。

关键词：DoS 攻击；动态防御；端信息跳变；插件

1 引言

近年来，随着全球数字化程度的不断提高，能源企业的网络安全也不可避免地呈现出了紧急态势。根据德勤的报告，能源行业已成为世界上第二个最容易遭受网络犯罪的行业。

能源企业信息系统的安全、稳定运行关系到民生国计和国家利益，网络攻防双方的对抗永远不会停止，由于新的技术、规则、漏洞接踵而至，导致沿用传统防火墙防护的企业，一般反应较慢，如果我们能够改变视角，关注自己，迫使黑客停止攻击，这将更加有效地减轻企业运维的负担，加快网络防护的反应速度。由此得到启发，如果我们自身的信息能够实现跳变，实施网络动态化的防御，将是一种有效的网络防御途径。

2 拒绝服务攻击简介

拒绝服务攻击（DoS）是通过占用诸如带宽、内存、CPU、磁盘空间等系统资源来阻止或弱化用户对网络、系统、应用的合法操作的攻击行为。一般 DoS 攻击的原理大致包含以下 3 个。①发生了大量突发数据流量，使得攻击对象的网络性能降低；②利用网络通信协议的特征，发送超过攻击对象处理能力的大量请求，以使得服务器不能向合法用户提供网络服务；③利用应用程序和操作系统自身存在的脆弱性，发送特殊结构的数据包，引起系统和软件的崩溃。

在网络层面，现有的网络防御系统通常采用防火墙、入侵检测、隔离网关、流量检测等多种软、硬件产品，对被保护网络进行网络攻击检测和防御。这些产品在一定程度上保护了网络的安全，在不断地发展和进步，然而，由于网络结构和配置方法固有的静态特性，这些防御技术的效用主要集中在增强网络静态对抗能力上。另一方面，检测攻击时依靠先验知识，而进行网络防御时很难防御内部伪五元组的数据流量，因此难以应对 DoS 攻击。

近年来，端信息跳变技术主要应用于主动防御中，同时受到越来越多的学者的关注，该技术可以看做是迷惑攻击者的动态蜜罐系统，它可以大大提高攻击者的时间成本，本文中实现了端信息跳变技术在 web 插件中的应用，经过测试，分析发现端信息跳变技术能够很好地防御 DoS 攻击。

3 端信息跳变防护技术原理

3.1 端信息跳变分类

从理论上讲，端信息跳变保护技术中的可跳变内容可以包括与端信息相关的各种元素，如端口、加密算法、地址甚至协议等。目前，相关研究成果和应用领域主要包括以下几个方面。

3.1.1 端口跳变

端口跳变技术是一种跳变思想，是近年来在网络安全领域内非常典型的应用。其主要原理是，在信息传输过程中，服务器服务的端口数随机变化，通信双方根据一定的同步策略传输信息。合法客户端可以跟踪服务器端口号的跳转以保持良好的同步以完成通信，而非法攻击者无法预测服务器在一个特定时刻使用的端口号，因此，无法获取所有通信内容或无法执行有效的攻击。

3.1.2 地址跳变

目前的大多数研究成果集中在一些 TCP 服务信号在通信过程中的动态变化，如 IP 和端口，以及使用端口结合地址跳变来抵抗 TCP 洪水攻击。

3.1.3 协议跳变

协议跳变是一种将大量可用协议预先存储在协议库中，包括网络通信协议和数据加密协议，在通信过程中通过在不同协议之间的跳变来动态选择下一个协议的技术。这种跳变形式不仅适用于两个节点之间的网络通信，也适用于设备中不同组件之间的数据传输。

3.1.4 混合跳变

混合跳变是一种结合了上述多种跳变的跳变技术。混合跳变具有更高的安全性能，可以有效减少攻击者的网络威胁。其中，snahe 代理跳变技术在使用代理的过程中采用了将地址跳变和协议跳变合二为一的混合跳变。

3.2 端信息跳变的核心技术

为了完成终端信息跳变的过程，需要重点解决跳变项选取、同步策略、网络服务切换技术和自适应策略的选择等问题，同时这些也是端信息跳变的核心技术。

3.2.1 跳变项选取

选取哪些端信息作为跳变项极为重要，跳变项的选

取直接决定了端跳变系统的安全性能以及服务性能。在因特网环境中，端信息的可跳变范围包括基本网络协议栈信息，例如端口、地址、协议。可跳变的端信息种类增加，通过组合使用，可以提供给服务器相关信息的跳变范围也变大，攻击者可以正确找到服务器位置的机会也更加渺茫，但这样也会加大整个系统的运行复杂性。

3.2.2 跳变同步方法

跳变同步方式与跳变服务的业务性能和安全性能密切相关。服务器端和客户端通过统一的同步策略从实现同步跳变通信。该技术部署后，攻击者将无法通过常用手段实现网络攻击，因为攻击者无法获得用户端信息跳变的规律。

3.2.3 网络服务切换技术

网络服务切换技术的重点是当网络服务从一个端信息切换到另一个时，如何确保服务的连续性。服务切换技术是实现端到端信息跳变的重要基础技术，其性能决定了端信息跳变系统的业务性能。目前已有成熟应用的转换技术，包括 Sochet 迁徙、跳变代理等技术。其中，跳变代理技术通过在客户端和服务器之间布置多个跳变代理，在跳变代理上实现跳变过程处理和跳变策略，并且在跳变代理之后隐藏真实的服务器。每个跳变代理具有独立的外部 IP 地址，并且可以接收和发送数据包。服务器的IP地址是内部IP地址,无法直接访问外部网络。客户需要通过同步模块获取服务器信息，并与相应的跳变代理进行通信。跳变代理可以将客户端的数据包转发给服务器，也可以将服务器的数据包转发给客户端，并且跳变代理可以在活动状态和非活动状态之间切换，只有活动状态的跳变代理可以进行转发工作，这使得客户端看起来像是在与一个 IP 地址和端口经常变化的服务器通信，但是服务器的真实 IP 地址和端口实际上是固定的。

3.2.4 自适应的跳变策略

端信息跳变技术通过动态变换和虚实交替的方式来应对网络攻击，最终目的是使攻击者失去攻击目标。因此，作为端信息跳变技术的重要组成部分，跳变策略应该能够动态变化，以应对复杂的网络环境和网络攻击的演变。

4 端信息跳变 web 插件部署

4.1 端信息跳变同步策略

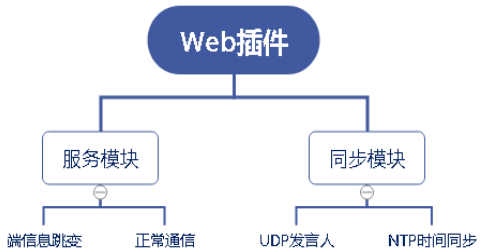

图 1 web 插件模型

能源企业在开展电子商务和网上远程访问业务时，需要经常使用 web 服务器，为了更好地抵御应用层针对 web 的 DoS 攻击，我们在信息中心的 web 服务器时引入了浏览器插件机制。使用插件的合法用户可以获得服务器的当前 IP 地址，而非法用户则不能。插件主要由两个模块构成，插件模型如图 1 所示。

由于 NTP 协议的部署方式简单，并具有高同步精度，我们在网络中配置了一个权威的 NTP 时间同步服务器，利用 NTP 协议实现网络时间同步。客户端和服务器端只有在时间同步的情况下才能进行通信。因此，web 服务器和插件必须定期与权威的 NTP 服务器同步时间，以便它们能够在短时间内保持精确的同步。UDP 发言人的功能是通知客户端当前系统的服务状态，例如在建立 TCP 连接时，客户端向服务器的 UDP 发言人发送时间戳请求。接收到时间戳请求后，UDP 发言人会将当前的时间戳返回给对应的客户端。

4.2 端信息跳变服务切换技术

插件的服务模块可以通过人工下达指令来改变其工作模式，正常通信模式下系统为用户提供正常的 web 访问功能。

在端信息跳变模式下，服务器的 IP 地址和端口号等信息进行持续跳变，对外客户的访问过程可以看作是客户端插件在和 N 个不同 IP 地址的虚拟服务器进行通信，每个虚拟服务器有且仅有一个 IP 地址和端口号，而且在同一时间只有一个虚拟服务器处于运行状态，端信息跳变网络通信模型如下图 2 所示：

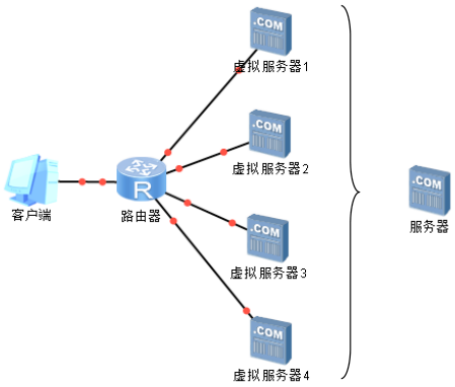

图 2 端信息跳变网络通信模型

上文提到服务切换技术是端信息跳变的核心技术之一，这里我们使用在客户端和服务器之间部署跳变代理来实现服务的切换，如图 2，服务器的 IP 地址为内部地址，外部的客户端无法直接访问服务器，必须通过跳变代理即虚拟服务器实现访问，每个虚拟服务器的 IP 地址都是独立的，并具有收发数据包的功能，客户端在发送访问请求的时候，首先通过图 1 中的同步模块从服务器获取相关信息，与对应的虚拟服务器进行通信，虚拟服务器在客户端和服务器之间完成数据转发。

4.3 插件性能分析

为了加大攻击者预测合法用户行为的难度，插件中端口、地址、协议等端信息需要进行伪随机跳变，使攻击者难以通过 DoS 攻击中造成有效的破坏；另一方面，对于截获攻击，由于服务器与跳变代理协同工作，攻击者捕获的信息是服务器信息伪随机变化后的数据包。这

使得攻击者很难将数据包进一步选择和排序，将它们解密成明文数据。

假设模型中端信息跳变可变地址数量为 n、可变端口数量为 m、可变协议数量为 k，则模型中可用的端信息跳变组合总共有 nmk 个。假设平均跳变间隙为 τ（即虚拟服务器和客户端插件的端信息每经过一个时间间隔 τ 就进行一次端信息跳变），当前时间为 t，由 INT（t/τ）计算得到当前时间单元号 i，因为在任意时刻只有一个跳变信息的组合，所以通过引进端信息跳变技术，可以知道攻击者的成功攻击时间 T' 为：

$$T'=T\left(1+\sum_{i=1}^{nmk-1}\left(i\frac{C_{nmk-1}^{i}}{C_{nmk-1}^{1}C_{nmk}^{i}}\right)\right) \quad (1)$$

其中，T 为没有使用端信息跳变技术时攻击者成功攻击所需要的时间，由式（1）可以看出，该模型抵御 DoS 的能力与可变地址数量 n、可变端口数量 m、可变协议数量 k 有关，还与平均跳变间隙 τ 有关，nmk 越大或 τ 越小，攻击者成功攻击耗费的时间 T' 就越长，系统性能越好。

5 抗攻击实验与结果分析

5.1 抗攻击实验设备环境

我们在完成端信息跳变 web 插件部署后，为了进一步测试插件抵御 DoS 攻击的能力，又在机房搭建了一个网络环境来模拟抗攻击实验。本次实验设备环境如下表 1 所示。

表 1 抗攻击实验设备环境

对象	主机系统	内存（GB）	处理器（GHz）	带宽（Mbit/s）
web 服务器	Linux	2	4.0	1000
客户端	Windows10	4	4.0	1000
攻击者	Linux	4	4.0	1000
NTP 服务器	Linux	2	4.0	100

实验中，安装 web 插件的客户端 IP 地址为 10.0.61.34，正常通信时，web 服务器的 IP 地址为 10.0.61.142，端口号为 8081，处于端信息跳变模式下，web 服务器地址从 10.0.61.140 到 10.0.61.149，端口从 10000 到 65535。

5.2 抗攻击实验结果及分析

实验过程中，我们模拟攻击者采用 SYN Flood 的方式对 web 服务器进行可控制、有指导的攻击。SYN Flood 的攻击原理是攻击者伪造真实客户的 IP 地址向 web 服务器发送大量的 SYN 报文，请求建立连接。由于攻击者的 IP 地址是伪造的，所以 web 服务器回应了 SYN 的回应报文（ACK）后，发送端并不会再继续回应 ACK 报文进行确认。这样 web 服务器的等待列表就会变得非常庞大，并且会不停地向伪造的真实客户（攻击者）发送用来回应 SYN 的 ACK 报文，占用着大量的资源无法释放。

但是我们在部署基于端信息跳变技术的 web 插件后，跳变代理会代替 web 服务器进行通信，且 IP 地址和端口号不断跳变，导致攻击者无法定位当前通信服务器所用的 IP 地址和端口号，成功防御 SYN Flood 攻击，避免了 web 服务器因资源消耗殆尽而崩溃。

由本次实验结果可知，随着攻击者攻击速率的不断增大，使用端信息跳变 web 插件时，web 服务器响应时间无明显增大，并逐渐趋于稳定。而没有使用 web 插件时，随着攻击者攻击速率的不断增大，web 服务器响应时间也不断增大。可见，这种基于端信息跳变技术的 web 插件能够分散网络中的流量，很好地防御了 SYN Flood 攻击。

6 结语

基于对能源企业各个业务的连续性和可用性的考虑，我们在企业总部信息中心的出口设置针对拒绝服务攻击的手段。将基于同步的端信息跳变技术应用于能源企业的 web 防护领域，通过双方协商统一的同步策略实施双方的端信息跳变，实现了用户在 web 访问中，能够主动抵御 DoS 攻击的功能，可见，对于能源企业来说，该技术与传统网络防护技术相比，具有很多优势。

6.1 抗攻击能力强

传统的网络保护技术在攻击的实施阶段和后续阶段进行防御，但端信息跳变技术在攻击的准备阶段就让非法攻击者失去了目标，无法定位服务器。基于这种端信息跳变的思想，通过结合诱惑和隐蔽的手段，可以有效地防止网络攻击。

6.2 抗截获能力强

在数据通信过程中，端信息的动态变化使得攻击者难以有效拦截数据包。由于网络拦截的目标通常是 IP 地址或本地网络，因此通常很难拦截更多不属于同一本地网络的数据通信。

但这种技术同步的实现比较复杂，在端信息变化过程中，需要通信双方的合作，而且端信息跳变的过程对合法用户也不透明，部署的难度较大。目前，对于端信息跳变自适应的研究还处于理论和原型系统验证阶段，与应用于真实的网络服务和应用部署还存在一定的差距，如果能够在自适应的跳变策略方面进一步研究，通过动态变换的方式应对网络攻击，将大大提升端信息跳变系统在网络防御中的能力。

参考文献：

[1] 李立勋，张斌，董书琴 . 网络动态防御体系下主机安全威胁分析方法 [J]. 网络与信息安全学报 ,2018,4(4):8.

[2] 刘江 . 网络动态防御策略及其有效性评估研究 [D]. 郑州：解放军信息工程大学 ,2017.

[3] 林楷，贾春福 . 基于消息篡改的端信息跳变技术 [J]. 通信学报 ,2013(12):142-148.

[4]HUANG Y, GHOSH A K. Introducing diversity and uncertainty to createmoving attack surfaces for web services[J].Springer New York,2011(11):131-151.

作者简介：

司凯文（1989- ），山西晋城人，男，本科，2012 年 7 月毕业于山西农业大学，工程师，研究方向：机电信息化。