UPnP 中的 DoS 攻击防御方案①

Scheme to Prevent Denial of Service Attacks on UPnP

王佳慧　贺　樑　（华东师范大学 计算机科学与技术系 上海 200241）

摘　要：针对通用即插即用（UPnP）服务中极易发生拒绝服务（DoS）攻击，本文提出了一种新的防御方案。该方案通过对 UPnP 结点设置带异常流量检测的包过滤和对 UPnP 控制结点设置基于规则的可扩展置标语言（XML）防火墙，分别限制了 UPnP 设备的连接数和基于应用层过滤了控制点所接收的无用描述信息，最终有效地防御了发生在 UPnP 中的 DoS 攻击。

关键词：通用即插即用 拒绝服务 可扩展置标语言防火墙 设备描述 服务描述

1 引言

随着数字家庭和网络的普及，数字家庭技术正日益成为现代数字主流技术。而 UPnP（通用即插即用）技术作为数字家庭技术的关键部分，使设备的智能互通成为可能，并简化了家庭或企业中智能设备的联网过程。然而，UPnP 引发的安全问题也接踵而来，其中防御由于 SSDP 被利用而引发的 DoS 攻击和 DDoS 攻击成为了众多用户和厂商共同研究的热点。目前，防御 DoS 攻击和 DDoS 攻击的方案层出不穷，它们用来防御各类网络环境下的拒绝服务攻击，而这些方案应用在数字家庭的这样的特定环境下并不完全适合。本文先对 UPnP 服务发现中的相关安全防御工作进行介绍，随后针对 UPnP 下 DoS 攻击和 DDoS 攻击的特点，提出了一种新的防御方案。

2 相关工作

UPnP 作为数字家庭的重要技术，在现实生活中被广泛应用。每台 Windows XP 都有默认的 UPnP 服务，而 UPnP 服务存在着严重的安全漏洞。其中一种就是 DoS，当发生此类攻击时，系统资源被大量占用，合法用户无法正常使用 UPnP 设备所提供的服务。

攻击者向具有 UPnP 服务的系统发起 DoS 攻击，主要的攻击情况主要有以下两种：一种是攻击者向 UPnP 设备发出攻击性的数据包，使得 UPnP 设备始终处于资源被大量占用状态。攻击者对用户系统发送 NOTIFY 指令，其中“LOCATION”域的地址指向另一个系统的 Chargen 端口，以便就具备 UPnP 服务功能的新设备进行广泛告知，并指示目标系统与 Chargen 服务器建立连接。于是，用户系统则向目标服务器发送下一条下载请求，而这仅仅是针对其所收到 NOTIFY 请求所给予的回应。另一种情况，当 UPnP 控制端对下载的设备和服务描述信息解析，而攻击性的信息常常伪装成合法的 UPnP 服务描述信息，引发用户系统产生 read/malloc 循环。

目前，为了防御此类攻击，微软针对不同的操作系统发布相应的下载补丁，或直接要求禁用 UPnP 服务选项。然而，这并不能积极主动地防御 DoS 攻击。包括 UPnP 在内的服务发现中极易发生安全性攻击，文献[1]介绍了一个基于特征（身份认证）的加密技术，实现保护用户的请求并且限制服务发现的访问，其主要局限在于该防御技术不能对抗攻击者对服务提供者发动的 DoS 攻击[1]。文献[2]则提出了一种有关服务发现的安全性服务的框架 SDS（Service Discovery Service）。这种集成的安全模型一方面提供保护敏感信息的服务，另一方面为用客户定位可信任服务。通过提供用户身份认证，授权，加密解密和访问权限控制机制来防御服务发现中的非法用户攻击和其他安全性问题。但是，SDS 不能主动地防御 DoS 攻击。

① 基金项目：上海市重大科技攻关项目（编号 06DZ15008），上海市科技人才计划项目（编号 07QB14036）

目前对抗 DoS 应用最广泛的是防火墙，它能有效地阻隔攻击源，从而主动地防御 DoS 攻击。用户在解析 XML 的服务描述信息时，可能因为其中隐含的攻击性信息而遭受 DoS 攻击。XML 防火墙对接受到的设备描述信息及其设备所带的服务描述信息进行检测，过滤。目前，流行的 XML 防火墙有 Forum XWall for ISA Server，DataPowerXS40 XML Security GateWay。XML 防火墙在安全方面的作用很明显，但是实现起来并不轻松。这主要是因为应用层安全本身就是比较复杂的问题，如果 XML 防火墙为每个 Web 服务提供一个包装，不仅工作量很大，而且不灵活，一旦安全策略发生改变，就要逐个修改每个 Web 服务的包装，这显然很繁琐而且容易出错。本文所做工作中最重要的一部分就是提取 UPnP 中发生 DoS 攻击的特性，设计一种基于规则的 XML 防火墙。

同时，对于 UPnP 设备频繁地接受连接而导致的内存资源大量消耗，本文设计了带异常流量检测的包过滤来限制 UPnP 设备的连接数。它是本文提出的防御机制中的另一个重要组成部分。

本文第三节详细描述了 UPnP 中 DoS 的防御方案，第四节对本文提出的防御方案进行实验分析，最后对全文进行了的总结。

3　UPnP 中的 DoS 攻击防御方案

3.1　UPnP 中的 DoS 攻击防御系统

WSA（Web Services Architecture）不同于 WWW（World Wide Web），前者的报文交换是以发送和接收服务为目的，后者是以获取信息为目的。DoS 攻击对于 UPnP 这种 WSA 中的服务发现来说，攻击通常发生在应用层。但仍不排除通过 Internet，UPnP 系统中会有来自传输层和 IP 层的 DoS 攻击发生。

DoS 攻击通过发送大量的无效数据包来占用用户有限的资源。在 DoS 攻击流量足够大的时候，无论 DoS 攻击是何种类型，都无法依靠隐藏和伪装来逃脱检查。同时，DoS 攻击不仅存在于 WSA，也可能来自 WWW。因此，增加一个初级的异常流量检测器是很有必要的 之后，通过一个包过滤器，达到有效限制工作结点的连接数的目的。接着判断该结点是否是 UPnP 控制点，如果是那么在包过滤之后还须经基于规则的 XML 防火墙过滤应用层的 XML 描述信息。UPnP 服务在防御系统中的工作流程如图 1 所示。

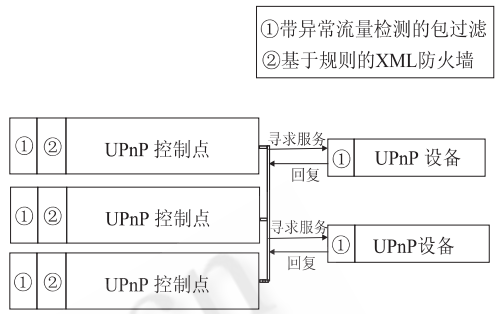

图 1　UPnP 服务在防御系统中的工作流程

3.2　带异常流量检测的包过滤

对长相关流量的 DoS 攻击的模式识别，误报漏报率低，算法简单，响应快[3]。待测流量的自相关函数 r_{yy} 与无攻击时正常流量自相关函数 r_{xx} 之差距，见式(1)，将与我们预定的阈值 V 进行比较。$\xi \geqslant V$，判为异常流量；反之，判为正常流量。$\Phi(.)$ 是误差函数，μ_ξ 和 σ 分别是序列的期望值与方差，根据式(2)，可求得 $p_i=1, p_f=0$ 的阈值 V 的范围。

$$\xi = \| r_{xx} - r_{yy} \| \tag{1}$$

$$V \in \left[-\sigma\Phi^{-1}(P_f), \mu_\xi - \sigma\Phi^{-1}(P_f) \right], \mu_\xi - \sigma\Phi^{-1}(i) > 0 \tag{2}$$

在异常流量检测后面设计了一个基于本机 CPU 负载监测的包过滤器。因为[4] 最后将可疑流彻底抛弃，而这容易丢失合法信息。所以，本文所做的改进，就是在异常流量检测器后面设计了一个基于本机 CPU 负载监测的包过滤器。依靠所提供的 CPU 负载，对可疑数据流循环判断检测，当确定受攻击用户 CPU 恢复到正常工作状态下周期性地动态更新，最后接收不再发动攻击的合法流。其流程图如图 2 所示。

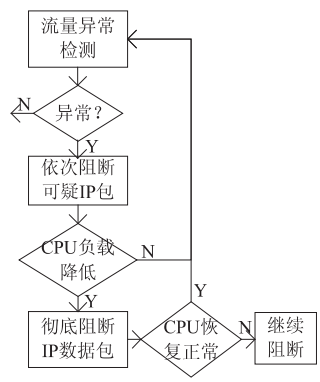

图 2　带异常流量检测的包过滤流程

3.3 基于规则的 XML 防火墙

由于 UPnP 控制点会对 UPnP 设备发送的 XML 形式表示的设备描述信息及设备所提供的服务描述信息解析。因此,当工作结点为 UPnP 控制点,且 UPnP 控制点收到 UPnP 设备回复后,需再经过一个 XML 防火墙的过滤(如图 1)。

究竟满足何种条件的描述语句才是合法的。这里我们列出 UPnP 中" 设备类型 "和" 服务类型" 的格式,设备类型的格式 :urn :schemas – upnp – org :device : uuid – device,uuid – device ;或 urn :domain – name : device :uuid – device,uuid – device," schemas – upnp – org "表示设备信息为工作委员会定义的," domain – name "字段为设备制造商注册的域名。服务类型是表示服务的统一资源名,一般格式 :urn :schemas – upnp – org :service :serviceType :version,或 urn : domain – name :service :serviceType :version,domain – name。根据以上的类型格式,抽象出设备描述语句必定包含(3)或(4),服务描述语句必定包含(5)或(6)。

urn :schemas – upnp – org :device : (3)

urn :domain – name :device : (4)

urn :schemas – upnp – org :service : (5)

urn :domain – name :service : (6)

在描述语句被 UPnP 控制点解析执行之前,先要判定接收到的设备及其服务信息的合法性,因此本文归纳了这些描述语句的特性从而提出了一个 UPnP 下的防火墙规则,图 3 用伪代码的方式显示了该规则。

```
if Node == UPnPControl //结点是UPnP控制点
    if(((3)∈ message) OR ((4) ∈ message))
    then access;
    if(((5)∈ message) OR ((6) ∈ message))
    then access;
else exit;
```

图 3　UPnP 控制点中的 XML 防火墙规则

新添加的规则实现了在 UPnP 控制点上的分流,合法的报文信息顺利地被控制点解析,执行 ;不合法的被防火墙阻断。带新规则的 XML 防火墙有效地实现了 UPnP 系统下对描述信息的合法检测。

4 实验分析

4.1 实验环境

为了评估该方案的性能,笔者将该文提出的方案与下面两种方案下面作比较 :异常流量入侵检测[5],每个结点都设置异常流量检测的包过滤和基于规则的 XML 防火墙的防御系统。实验以 SSFNET 作为网络仿真平台。实验环境是一台具有 2G 内存和双 1.73GHz CPU 的 Windows XP Professional 服务器。网络结点包括三个 UPnP 控制点,两个 UPnP 设备,距离目标 14 跳有一个攻击源间断性地发送攻击性的描述信息给 UPnP 设备。同时,攻击源也可能伪装成 UPnP 设备,通过向 UPnP 控制点发送不合法的服务描述信息以发动 DoS 攻击。

4.2 性能测试

(1) 攻击包过滤精确度的测试。此试验中,为了将原有复杂的试验简化,可以将单攻击源 A 伪装成合法 UPnP 设备和 3 个 UPnP 控制点进行 DoS 攻击仿真试验。列表 1 显示了在攻击流量为 10000packets/s 和 10packets/s 时,文献[5] 和本文提出方案分别过滤的攻击包占实际发放攻击包总数的百分比,在这里我们将这个百分比定义为攻击包过滤精确度。通过对表 1 的观察我们可以得出,大流量 DoS 攻击发生时,两个方案攻击包过滤精确度都很高 ;而小流量 DoS 攻击,文献[5] 攻击包过滤的精确度非常低,而本方案仍旧具备很高的过滤性。这点是可以理解的,因为[5] 的门限算法对于高强度攻击性能很好,但对于低强度攻击,监测效果就变得很差,误报率和漏报率明显上升[6]。而本文提出的基于规则的 XML 防火墙,在应用层对数据包逐个检测,因而有效防御了小流量的 DoS 攻击。

表 1　防御系统过滤攻击包的精确度

	10000 (packets/s)	10 (packets/s)
文献[13]	90.03 %	9.31%
本文方案	83.13%	83.11%

(2) 过滤效率(单位时间内过滤攻击包数)的测试。本文仅在 UPnP 控制点上设置 XML 防火墙,源于 XML 防火墙处理时间相对于工作在网络层和传输层的防火墙工作时间长很多。通过本试验的仿真试验数据得出,有选择地设置基于规则的 XML 防火墙以及所有防御设置在结点进入工作状态时动态触发,与无选择地将所有结点都设置各项防御设备相比,平均速率提高了 21.03%。由此体现了在 UPnP 系统中本文设计

的防御系统的合理性和灵活性,这使得防御系统的工作效率大大提高。

5 小结

对于 UPnP 服务中极易发生的 DoS 攻击,本文提出了一种新的防御方案,它包括两个组成部分:带异常流量检测的包过滤,基于规则的 XML 防火墙。其中,前者限制了 UPnP 设备的连接数,将获取的异常流量数据包在反复检测的情况下进行过滤。后者由 UPnP 控制点进入工作状态时刻动态启用,基于应用层过滤了接收到的无用描述信息。

本文提出的防御方案在 UPnP 环境中具有防御小流量 DoS 攻击时包过滤精确度较高,防御效率较高的优点。由于 XML 防火墙工作在应用层,因此解析报文所花费的时间较工作在 IP 层和 TCP 层的防火墙要长。实验数据表明,XML 防火墙每秒最多可以处理不超过 300 消息[7,8]。但对于像家庭,小企业此类布局较为简单的局域网环境,可以通过实施本文所提出的方案来有效防御 UPnP 中的 DoS 攻击。

参考文献

1 Slim Trabelsi, Jean – Christphe Pazzaglia, Yves Roudier. Secure Web Service discovery: overcoming challenges of ubiquitous computing. Proceeding of the European Conference on Web Services (ECOWS'06), 2006:35 – 43.

2 Steven E. Czerwinski, Ben Y. Zhao, Todd D, Anthony D, Randy H. Katz. An Architecture for a Secure Service Discovery Service. In: Fifth Annual International Conference on Mobile Computing and Network, Seattle, WA, 1999 – 08:256 – 264.

3 Lin CY, Wu M. Rotation Scale and Translation Resilient Watermarking for Images. IEEE Transactions on Image Processing, 2001, 10 (5):765 – 782.

4 程勇,秦祖福,傅建明. 有序二叉树在防火墙规则库中的应用. 武汉大学学报(理学版). 2006, 52 (1): 77 – 80.

5 Siris, VA, Papagalou F. Application of anomaly detection algorithms for detecting SYN flooding attacks. In: Proc. of the Conf. on Global Telecommunications (GLOBECOM). IEEE, 2004. 2050 – 2054.

6 孙知信,唐益慰,程媛. 基于改进 CUSUM 算法的路由器异常流量检测. 软件学报, 2005, 16 (12): 2118 – 2122.

7 Frederic Avolio. Firewalls and Internet Security, the Second Hundred (Internet) Years. Internet Protocol Journal, Cisco Systems, and Jun 1999, 2 (2):10.

8 Ying – Dar Lin, Huan – YunWei, and Shao – Tang Yu. Building an Integrated Security Gateway: Mechanisms, Performance Evaluation, Implementation, and Research Issues. IEEE Communication Surveys and Tutorials, Vol. 4, No. 1, third quarter, 2002.