一种基于信令流阻断的 SPIT 的检测和阻止方法

A new method of SPIT detection and prevention based on the broken of signaling

赵 凯 朱罡华 辛 阳 杨义先 钮心忻
(北京邮电大学信息安全中心 100876)
(北京邮电大学网络与交换技术国家重点实验室 100876)

摘要:本文给出了下一代网络中一种新的 SPIT 的检测和阻止方法,该方法应用于 IP 多媒体子系统结构,在信令流检测和恶意用户举报的基础上,采用信令流阻断的方法能够很好的检测和阻止 SPIT 的传播。

关键词:下一代网络 IP 多媒体子系统 SPIT 信令流检测

1 引言

SPIT (SPAM OVER INTERNET TELEPHONE)广义上定义为多媒体垃圾,即下一代网络中基于语音、视频、立即消息或别的形式的垃圾信息。在今天互联网饱受 SPAM 垃圾邮件肆虐的同时,为了吸取垃圾邮件危害社会后再去治理的教训,在下一代网络蓬勃发展的同时,SPIT 的检测和阻止已经成为下一代网络中 IP 多媒体子系统(IMS)[1]在未来安全工作中的一项重要任务。

IP 多媒体子系统采用 SIP 协议[2]进行端到端的控制,同时支持固定和移动的接入。国际电信联盟已经将 IP 多媒体子系统作为 NGN 核心网基于 SIP 会话的子系统的基本架构。SPIT 在某种意义上可以视为传统的 SPAM 在 IP 多媒体子系统中的应用,按照 SPIT 消息产生的方式,IP 多媒体子系统中存在以下三种 SPIT 信息:

呼叫(CALL SPAM):攻击者主动发起呼叫请求,试图建立一次语音、视频、立即消息或别的通信,一旦用户响应,攻击者便会通过媒体通道发送大量的垃圾语音信息。

立即消息(IM SPAM):同垃圾邮件一样,攻击者向用户发送大量的包含垃圾信息的立即消息。IM SPAM 一般使用 SIP Message 发送,因此这种垃圾信息可以出现在任何具有来电显示功能的终端上。如 SIP INVITE 请求中包含大的 SUBJECT 头域,或 INVITE 消息包含文本或 HTML 消息体。

存在(PRESENCE SPAM):和立即消息一样,这种 SPIT 是指攻击者发送大量的 PREENCE 请求,如 SUBSCRIBE 请求 PRESENCE 事件包等,试图获得用户的好友列表或白名单,从而向他们发送垃圾消息。

由于目前还没有一个好的方案能够很好的解决垃圾邮件的问题,因此 SPIT 的检测和阻止已经成为业界研究的重点和难点。本文的组织如下,在第二部分介绍了 SPIT 的研究现状,然后介绍一种新的基于信令流阻断的 SPIT 的检测和阻止框架,在第四部分介绍了系统的检测和阻止原理,第五部分给出了一个应用实例,最后就 SPIT 的检测和阻止给出了进一步的思考。

2 研究现状

目前的反多媒体垃圾技术多是借鉴反垃圾邮件的研究成果[3],包括内容过滤、黑名单、白名单、基于内容的通信、名誉系统、地址混乱、限制用户地址、图灵机测试、谜语计算、风险付费以及发送方检测等。由于下一代网络中多媒体通信的特殊性,和反垃圾邮件相比这些方些用在 SIP 协议上都有一定的局限性,如内容过滤几乎对网络电话没有任何作用,首先用户响应呼叫的时候,信令通道和媒体通道都已经建立,垃圾信息如语音或图像信息已经传递到用户端或以某种方式已经存储,但是目前的技术还不能分析出语音或图像是否是垃圾信息,给检测带来很大的局限性。

和互连网接入的开放性相比,下一代网络的接入需要严格的身份认证,因此问题解决的关键是发送方

的身份识别，IP 多媒体子系统中，SIP 协议采用 HTTP DIGEST 认证，但是这种认证是一种单向认证，容易受到服务器的欺骗攻击，同时也存在有一定的脆弱性如离线字典攻击。目前比较好的方法是西门子提出的基于安全声明标识语言（SAML）的检测和阻止方法[4]，该方法采用域用户认证的方式，即一旦一个域认证自己的用户后，如果该用户想和别的域进行通信时，发送域方需要声称身份，并要对有效性进行数字签名，这样做的前提条件是各个域之间要相互信任。

上述解决方法都是基于用户的身份认证，本文给出了一种新的基于信令流阻断的检测方法，该方法综合信令流检测和恶意用户举报，采用服务器间联动的方式很好的检测和阻止 SPIT 的传播。

3 系统组成

基于信令流阻断的 SPIT 检测和阻止系统主要由由监控终端、策略服务器、代理呼叫会话控制（P－CSCF）、查询呼叫会话控制（I－CSCF）、服务会话控制（S－CSCF）以及归属服务器（HSS）等组成。如下图 1 所示，各部分间联合作用共同完成 SPIT 的检测和阻止。

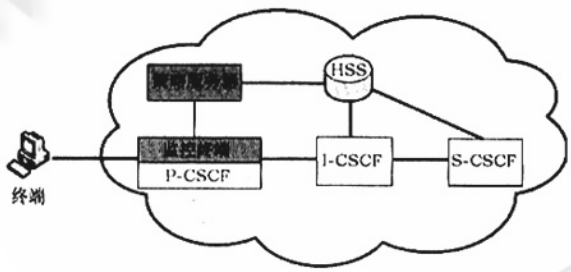

图 1　系统组成

监控终端：完成 SPIT 信令流的检测和恶意用户的举报功能，位于核心网络边界，直接和终端用户接口，既可以是位于 P－CSSF 前的一个独立的物理设备，也可以是一个逻辑设备嵌入到 P－CSCF 中。

策略服务器：根据监控终端发来的恶意用户名单，完成用户策略的制定，控制 HSS 归属服务器中用的信任级别，从而达到限制用户服务的目的。

P－CSCF：主要实现代理服务器的功能，同时也可以实现用户代理（UA）的功能。P－CSCF 根据主叫/被叫 SIP 的通用资源标识符（URI）查询相应的归属域，完成用户的注册和呼叫连接。

I－CSCF 是 P－CSCF 和归属域的连接点，根据用户属性在归属用户服务器（HSS）中查询相应的 S－CSCF 来为该用户服务。

S－CSCF 具有 SIP 登记员和 SIP 代理服务器的功能，是整个 IMS 系统的控制核心。SIP 登记员接受用户的注册请求并记录用户的 SIP 地址和 IP 地址，SIP 代理服务器提供路由功能并负责将 SIP 用户请求和响应前转到相应的下一跳。同时 S－CSCF 还具有 UA 的功能。

归属用户服务器（HSS）是用户数据库系统，支持网络实体处理呼叫/会话的包含签约信息的实体包含了 IMS 用户鉴权和会话建立所需的所有用户数据。存放着用户的认证信息、用户的信任信息和业务受限信息、用户的业务信息、用户的漫游信息等。

4 检测和阻止过程

4.1 SPIT 的检测

SPIT 的检测主要由监控终端完成，当恶意用户发起 SPIT 呼叫时，信令流会首先通过监控终端，此时信令流检测程序会对进出的信令流进行分析，利用 SPIT 检测算法判断是否为 SPIT 呼叫信令，对于 SPIT 呼叫信令，会向呼叫者回送一个拒绝信息，同时提取呼叫方的用户信息送到策略服务器，修改该用户的信任信息。这种方法目前主要用于检测机器群发。

同时终端用户可以通过监控终端举报一些恶意用户，这种情况主要是一些恐吓内容或骚扰信息，这些消息一般都是正常的信令流，但是会给用户带来一定的危害，用户受到第一次危害后可以立即将恶意用户信息发给监控终端，由监控终端完成后续的工作。

4.2 用户信任管理

用户信任信息的管理是由策略服务器完成的。在用户归属服务器中，除了存放有用户的认证信息、业务信息和漫游信息外，还为每个注册用户添加了信任信息和业务受限信息。其中用户的信任信息包括普通、警告、监控和业务受限等四种情况。

用户在开始注册时会检查信任信息，如果是一个新用户其信任级别定为普通，如果是业务受限则会拒绝其注册网络。一般情况下通过信令流检测出的 SPIT 用户或举报的恶意用户其信任信息定为警告，同时会发送相应的警告信息给用户，提请注意。对于一个域

内的多个用户同时举报一个恶意用户，直接将这个恶意用户的信任信息定义为监控，如果情节恶劣则取消该用户的业务，发送业务受限信息。

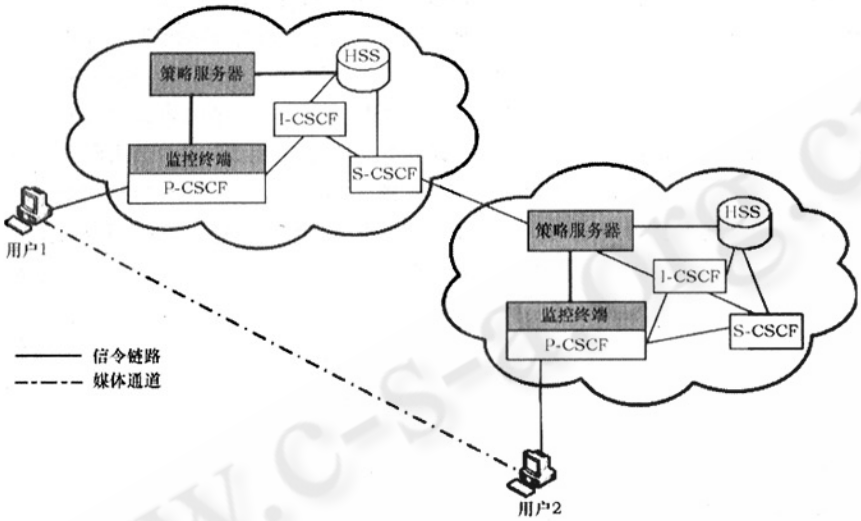

图 2　SPIT 检测和阻止应用实例

户，各个域间的归属服务器还会定时交换恶意用户信息。如果本域内处于监控状态的用户出现在别的域的恶意用户名单上，则会对其进行业务受限处理。

4.3 SPIT 的阻止

和垃圾邮件的传输不同，SPIT 的成功传输是建立在信令流的基础上，即首先发送端要和接收端建立信令链路，协商媒体信息，然后开始媒体流传输。因此如果将通信双方的信令流阻断，媒体通道就不可能建立起来，更谈不上 SPIT 的传输。

信令流的阻断是建立在检测的基础上，由 S－CSCF 来完成的。当用户注册时，S－CSCF 会通过归属服务器检查用户的信任信息，如果是警告或监控状态会通知用

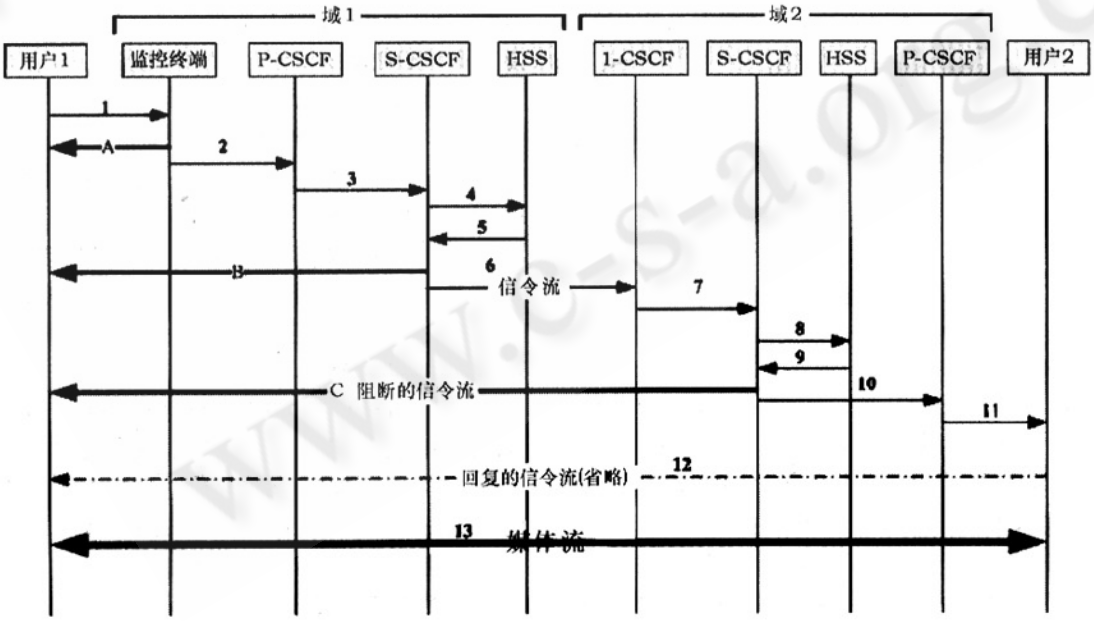

图 3　用户一次会话流程

同时在用户归属服务器中还存放有用户举报的别的域的恶意用户信息。为了防止骚扰本域内的用户注意，如果处于业务受限状态，会回送用户注册不成功消息。在会话中一方面通过信令流检测来阻止 SPIT

信令流,同时结合用户举报信息利用 S－CSCF 来阻断 SPIT 信令流的建立。

5 应用实例

下图给出了基于信令流阻断的 SPIT 检测和阻止系统的应用实例。应用环境如下图 2 所示,域 1 内的用户 1 企图和域 2 内的用户 2 通信,这里介绍的是跨域通信的情况,单个域内的通信处理机制是一样的。

在应用过程中可以有以下几种情况:二者正常通信;用户 1 发送 SPIT 信息;用户 1 业务受限;用户 1 在域 2 内的黑名单内。为了更好的说明问题,给出了二者通信的信令流和媒体流建立过程,如图 3 所示。

(1) 正常通信流程。正常通信时,如图所示,红色部分1到12表示信令流的建立过程,其中用户 2 向用户 1 回复的信令流用信令流 12 代表了,在双方信令流完成后,双方的能力协商已经完成,媒体通道也已经建立,下面就可以正常的传输语音、视频或别的多媒体信息了。

(2) 用户 1 发送 SPIT 信息。当用户 1 发送 SPIT 信息时,如发送广告信息,这时域 1 内的监控终端会对进入网络的信令流进行检测,如果发现是用户 1 发送 SPIT 信息,则会在向其回复一个警告信息,同时中断此次通信如黑色信令流 A 所示,同时将用户 1 的信任信息该为警告。

(3) 用户 1 业务受限。当用户 1 业务受限时,在其注册时系统会回复注册失败的消息,如图中黑色的信令流 B 所示,此时用户 1 不能享用网络服务,需要找运营商处理,防止了其进一步危害。

(4) 用户 1 在黑名单中。如果用户 1 在域 2 的黑名单中,则当域 1 内的 S－CSCF 将呼叫信息转到域 2 时,域 2 内的 S－CECF 会检测黑名单,如果发现用户 1 在黑名单中会回复一个呼叫失败的消息给用户 1 如黑色信令流 C 所示。

6 结束语

如何更好的识别 SPIT 信令流即 SPIT 信令流检测算法的准确性是需要进一步研究的问题。对于用户信任管理的问题也需要进一步深入研究。

参考文献

1 3GPP2 TS 23. 228 : "IP Multimedia Subsystem (IMS)"

2 Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

3 Rosenberg, J., Jennings. C, The Session Initiation Protocol (SIP) and Spam draft－ietf－sipping－spam－01 July 17, 2005.

4 D. Schwartz B. Sterman draft－schwartz－sipping－spit－saml－00. txt October 17, 2005.