第33卷 第12期 计 算 机 工 程 2007年6月
Vol.33 No.12 Computer Engineering June 2007
·安全技术· 文章编号：1000—3428(2007)12—0163—03 文献标识码：A 中图分类号：TP393

一种新的SPIT检测和阻止方法

赵 凯[1,2]，朱罡华[1,2]，辛 阳[1,2]，杨义先[1,2]，钮心忻[1,2]
（1. 北京邮电大学信息安全中心，北京 100876；2. 北京邮电大学网络与交换技术国家重点实验室，北京 100876）

摘 要：SPIT检测方法多是采用垃圾邮件的检测方法，有很大的局限性。该文给出了一种应用于IP多媒体子系统结构中新的SPIT的检测和阻止方法，该方法基于黑名单和信令流双重检测，采用信令链路阻断的方法能够很好地检测和阻止SPIT的传播。
关键词：IP多媒体子系统；SPIT；黑名单；信令流检测

A New Method of SPIT Detection and Prevention

ZHAO Kai[1,2], ZHU Ganghua[1,2], XIN Yang[1,2], YANG Yixian[1,2], NIU Xinxin[1,2]
(1. Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876;
2. State Key Laboratory of Networking and Switching, Beijing University of Posts and Telecommunications, Beijing 100876)

【Abstract】The methods used in SPAM detection which are adopted in SPIT detection so far have too many limits. This paper presents a new method of SPIT detection and prevention in NGN. This method is based on the detection of signaling and black lists in IP multimedia subsystem. And the broken of signaling is used to detect and prevent SPIT.
【Key words】IP multimedia subsystem (IMS); SPIT; Blacklist; Signaling-detection

在下一代网络中恶意用户会发起类似垃圾邮件的行为即SPIT(spam over internet telephone)，广义上称为多媒体垃圾，这种行为主要是针对SIP协议的。发起者可以利用SIP协议发起呼叫，企图和目标用户建立语音、视频或别的会话，也可以发起大量无用的即时消息(instant message)，这种攻击效果和垃圾邮件一样；甚至也会发起PRESENCE攻击，企图登上用户的白名单或用户列表，从而向对方发送垃圾信息。

目前的SPIT发送方式有以下2种：

(1)机器发送方式，即发起者首先录制好一段音频或视频，典型的如广告信息，然后收集用户的SIP URI地址或电话号码，通过和受害者建立会话连接达到目的，通常可以使用几台PC机来完成，机器内安装有通信软件，可以24小时连续服务。这种方式具有发送消息数量大、间隔时间短、效率高、受害面积广等特点。

(2)通过人工发送SPIT消息，即个人或群体通过单独和目标用户建立会话连接，达到一定的目的，同机器发送相比这种方式具有目的性强、鉴别困难等特点。

由于目前还没有一个方案能很好地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。

1 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[1]，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，这些方法用在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，首先用户响应呼叫时，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。

和互联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[2]。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多种机制联合作用的检测方法，该方法综合信令流和黑名单联合检测，通过信令链路阻止很好的检测和阻止SPIT的传播。

2 SPIT行为模式分析

和一般的攻击相比，SPIT的传送是建立在正确的行为基础上，即具有正确的呼叫路由和呼叫信令，其目的就是希望对方能正常接收信息，因此，检测具有很大的难度。总的来说，SPIT具有如下几种行为模式：

(1)短时通话

这种方式和正常的通话相比，SPIT一般通话时间比较短，通话建立后，发起者会急于向目的方播放或宣传垃圾信息或骚扰信息，达到目的后就会终止通话，因此通话时间比较短。

作者简介：赵 凯(1977－)，男，博士生，主研方向：下一代网络安全；朱罡华，硕士生；辛 阳，博士、讲师；杨义先、钮心忻，博士、教授
收稿日期：2006-08-07 **E-mail：**buptzk@163.com

(2)两次通话间隔短

SPIT 发起者的目的主要是广告，需要面向更多的用户，因此，相邻通话时间会很短，即向一个目标用户发送完信息后，紧接着会和另一个目标用户联系。

(3)呼叫不存在的用户

这种方式和垃圾邮件相似，SPIT 的发起者事先会收集许多用户地址信息如 SIP URI 或电话号码，这些地址信息有些是有效的，有些是无效的。

(4)第三方呼叫

这种方式是 SPIT 发起者向目标发送一个 REFER 消息，指向一个事先录制好多媒体广告信息的链接，一旦用户建立连接就会收到垃圾信息。

(5)关系呼叫

这种方式是主叫和被叫之间的关系，有时候主叫偶尔打错电话，或是双方通话内容简单，这种比较难判断，一般需要被叫用户配合。

3 系统组成

基于信令流检测和黑名单双重检测的 SPIT 检测和阻止系统主要由由监控终端、用户管理、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。

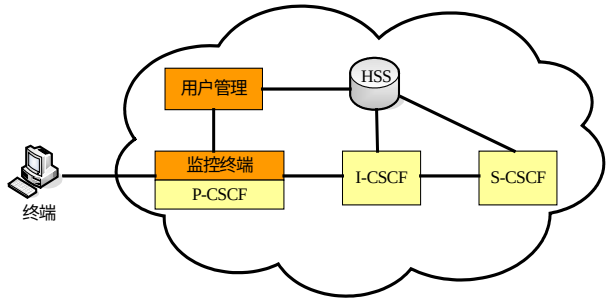

图 1 系统组成

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。

用户管理里面存有用户黑名单，同时根据监控终端发来的用户信息，计算用户的名誉值，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

(1)SPIT 的检测

SPIT 的检测主要由监控终端和用户管理共同完成，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用户管理单元，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。

(2)用户管理

用户管理的主要功能是在信令流检测中提供黑名单信息，同时在信令流检测的基础上计算用户的名誉值。黑名单的来源有 1 种方式：(1)通过终端用户的举报，如一个域内的多个用户同时举报一个恶意用户，则可以将这个恶意用户直接放入黑名单；(2)通过信令流进行检测，通过计算用户的信任值，如果用户的信任值降低到一定级别，就会考虑将该用户放入黑名单。

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 4 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放到黑名单中，发送业务受限信息。

(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，就不可能建立媒体通道和 SPIT 的传输。

SPIT 的阻止建立在信令流检测和动态黑名单基础上，即通过信令流检测算法，参考用户管理中的黑名单，从信令链路上中止 SPIT 信息的进一步传送。

5 应用实例

图 2 给出了基于信令流检测和黑名单双重检测的 SPIT 检测和阻止系统的典型应用实例。在这种应用环境情况下，用户 1 通过一台 PC 机进行向 PSTN 内的用户发送 SPIT 信息。在应用过程中考虑了以下几种情况：二者正常通信；用户 1 发送 SPIT 信息；用户 1 业务受限；用户 1 在黑名单内。图 3 从会话过程出发详细描述了 SPIT 信息的检测和阻止过程。

(1)正常通信流程

正常通信时，监控终端首先会对信令流进行检测，同时根据用户管理提供的黑名单进行过滤，如果是正常用户则会

正常通信。图 3 中 1~9 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 9 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。

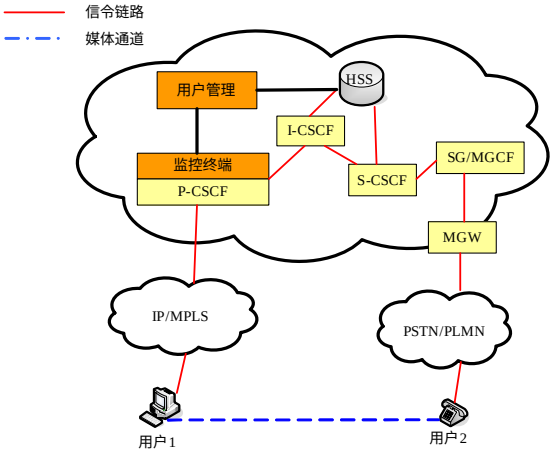

图 2 SPIT 检测和阻止应用实例

(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 1 个警告信息，同时中断此次通信如黑色信令流 A 所示，并将用户 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 3 中信令流 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 在本域的黑名单中，监控终端会在用户管理模块提供的黑名单中发现此用户，系统会回复一个呼叫失败的消息给用户 1，如图 3 中信令流 A 所示。

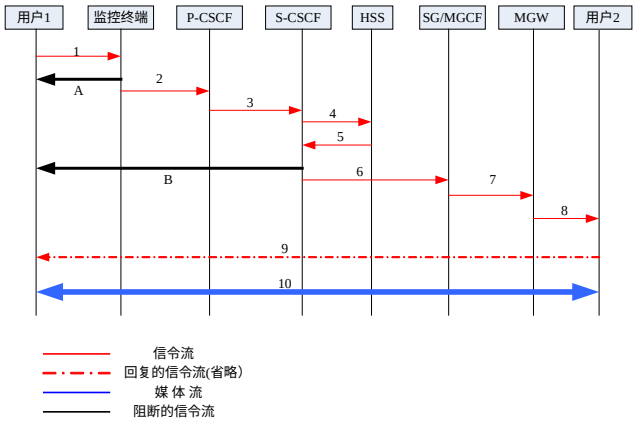

图 3 SPIT 检测和阻止过程

6 结束语

本文基于信令流检测和黑名单双重检测的 SPIT 的检测和阻止方法有效地结合了 2 种检测算法的优点，同时避免了其不足。但信令流检测算法的准确性是需要进一步研究的问题，同时，对于用户信任管理的问题也需要进一步深入的研究，尤其是处理用户陷害的问题，即恶意用户采用欺骗信息来陷害合法用户等。

参考文献

1 Rosenberg J, Jennings C. The Session Initiation Protocol (SIP) and Spam[Z]. draft-ietf-sipping-spam-01, 2005.

2 D Schwartz, Sterman B. SPAM for Internet Telephone (SPIT) Prevention Using the Security Assertion Markup Language (SAML) [Z]. draft-schwartz-sipping-spit-saml-00.txt, 2005.

(上接第 159 页)

2 Jackobsson M, Impagliazzo K R. Designated Verifier Proofs and Their Applications[C]//Proc. of Cryptology-Eurocrypt. Springer-Verlag, 1996: 143-154.

3 Steinfeld R, Bull L, Pieprzyk H J. Universal-verifier Signatures[C]// Proc. of Cryptology-Asiacrypt. Springer-Verlag, 2003: 523-542.

4 Cheng Xiaofeng, Zhang Fangguo, Kim K. Limited Verifier Signature from Bilinear Pairings[C]//Proc. of ACISP. 2004: 313-324.

5 Araki S, Uehara S, Imamura K. The Limited Verifier Signatures and Its Application[J]. IEICE Trans. on Fundamentals, 1999, E82-A(1): 63-68.

6 Boneh D, Lynn B, Shacham H. Short Signatures from the Weil Pairings[C]//Proc. of Cryptology-Asiacrypt. Springer-Verlag, 2001: 514-532.

7 Boyen X. Multipurpose Identity-based Signcryption: A Swiss Army Knife for Identity-based Cryptography[C]//Proc. of Cryptology. Springer-Verlag, 2003: 382-398.

8 Zhang Fangguo, Kim K. A Universal Forgery on Convertible Limited Verifier Signature Scheme[J]. IEICE Trans. on Fundamentals, 2003, E86-A (2): 515-516.

(上接第 162 页)

参考文献

1 Trusted Computing Group(TCG). TCG Trusted Network Connect TNC Architecture for Interoperability Specification (Version 1.0)[Z]. 2005-03.

2 宁宇鹏, 陈　昕. PKI 技术[M]. 北京: 机械工业出版社, 2004.

3 Trusted Computing Group(TCG). TCG PC Client Specific TPM Interface Specification (Version 1.2)[Z]. 2005-11.

4 万　涛. 网络中身份认证技术的研究[D]. 西安: 西安电子科技大学, 2003-01.

5 朱雁辉. 防火墙与网络封包截获技术[M]. 北京: 电子工业出版社, 2002-07.

6 李志民. 基于密钥的安全认证系统设计[J]. 中原工学学报, 2004, 15(6).

7 Trusted Computing Group (TCG). TCG Specification Architecture Overview Specification(Revision 1.2)[Z]. 2004-04.