基于 Fuzz 测试的 IMS 网络 SIP 漏洞挖掘模型*

刘树新，彭建华，刘彩霞，谢晓龙
（信息工程大学 国家数字交换系统工程技术研究中心，郑州 450002）

摘　要： 为有效挖掘 3G 核心网 IP 多媒体子系统中 SIP 流程存在的安全漏洞，提出了一种基于 Fuzz 测试的 SIP 漏洞挖掘模型。基于 Fuzz 漏洞测试方法设计了一种 SIP 漏洞挖掘模型，设计的初始消息状态转移方法实现了其中的消息注入功能，使漏洞挖掘进入到 SIP 流程内部，实现了自适应监控功能，针对不同监控内容实施相应的监控方法。仿真结果验证了模型及其功能方法的有效性。

关键词： 漏洞挖掘；模糊；会话初始协议；IP 多媒体子系统
中图分类号： TP393.08　　**文献标志码：** A　　**文章编号：** 1001-3695(2012)09-3456-04
doi:10.3969/j.issn.1001-3695.2012.09.068

SIP vulnerability discovery model in IMS based on Fuzz testing

LIU Shu-xin, PENG Jian-hua, LIU Cai-xia, XIE Xiao-long
(*National Digital Switching System Engineering & Technological Research Center*, *Information Engineering University*, *Zhengzhou* 450002, *China*)

Abstract: To effectively discover the vulnerability in the communication process of SIP protocol in the IP multimedia subsystem of 3G core network, this paper proposed a vulnerability discovery model. Firstly, this paper designed a SIP protocol vulnerability discovery model based on the Fuzz vulnerability testing. Then it designed states transfer method of initial message to achieve the message injection function of the model. Finally, it realized the seft-adaption monitoring function in the model, which could implement relevant monitor methods according to different monitor objects. Simulation experimental results show the effectiveness of the vulnerability discovery model and its function achievement.

Key words: vulnerability discovery; Fuzz; SIP; IMS

IP 多媒体子系统(IP multimedia subsystem,IMS)是传统电信网和互联网融合的重要部分,为未来的各种多媒体数据业务提供了一个通用平台[1]。会话初始协议(session initiation protocol,SIP) 是 IMS 网络的会话控制协议,主要用来建立、修改和终止多媒体会话过程。SIP 的安全性是 IMS 网络安全问题的核心。

目前,有关 SIP 安全问题的研究主要集中在 IMS 网络异常检测和安全测试方面。文献[1~3]研究了 IMS 网络中存在的 SIP 洪泛攻击的检测方法;文献[4]提出了一种 SIP 测试方法,向 SIP 软终端中注入混杂的 SIP 消息,挖掘基于 SIP 的 VOIP 软终端的安全漏洞;文献[5]利用 PROTOS 测试工具向 IMS 架构注入大量的异常 INVITE 消息,检测网络的鲁棒性和安全级别。但是,对 SIP 正常流程中可能存在的安全漏洞,还未见相关文献有所研究。针对以上问题,本文提出了一种基于模糊(fuzz)测试[6]的 IMS 网络 SIP 流程漏洞挖掘模型。

1　基于 Fuzz 的 SIP 流程漏洞挖掘模型

图 1 显示了 IMS 网络中主要的呼叫/会话控制功能实体(call/session control function, CSCF),包括代理 CSCF(P-CSCF)、问询 CSCF(I-CSCF)、服务 CSCF(S-CSCF)[7],共同完成 IMS 网络的会话控制。

SIP 主要负责 CSCF 之间的通信,其协议流程如图 2 所示。

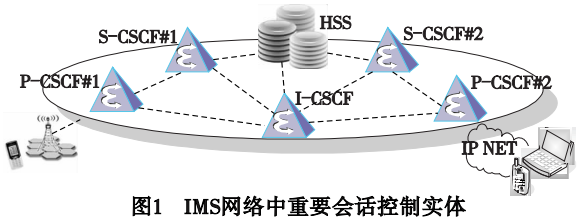


图1　IMS网络中重要会话控制实体

其中,图 2(a)是用户的注册流程,流程中的请求和响应相互配对:用户发送 register#1 消息至 P-CSCF、I-CSCF、S-CSCF 进行注册,S-CSCF 对用户发起鉴权返回 401 消息,用户接收消息后再次发送带有鉴权响应信息的 register#2 至 S-CSCF 鉴权完毕,用户收到 200 OK 完成注册流程。图 2(b)的会话流程与(a)同理。

对 SIP 流程特点进一步分析,可把消息流程抽象为如图 3 所示的流程实体收发链。其中,节点 $0-n$ 是流程中的 $n+1$ 个通信实体;S_0 为流程中的初始消息;S_i 为流程中节点 $i-1$ 发送至节点 i 的消息;R_i 为节点 i 发送至节点 $i-1$ 的响应消息。$\{S_i, R_i\}, i=0,\cdots n$ 表示一个完整 SIP 消息所包含的 SIP 消息字段的集合,SIP 消息字段是集合中的某个元素。

可见,每个 SIP 流程需要多个实体参与,这些实体对消息中消息字段的修改或恶意转发都可能对 IMS 网络的安全造成威胁。在 IMS 网络中,SIP 流程主要存在以下安全问题[8]:

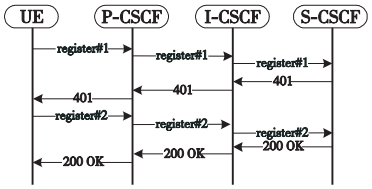
a)消息字段修改。攻击者可以模拟流程中的消息修改相

收稿日期: 2012-02-23;**修回日期:** 2012-03-26　　**基金项目:** 国家"863"计划资助项目(2011AA010604,2008AA011003)

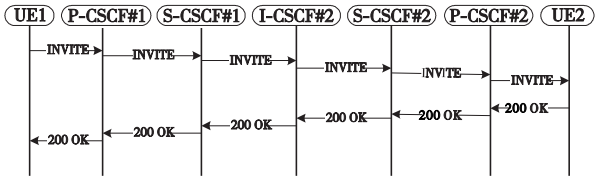
作者简介: 刘树新(1987-),男,山东潍坊人,硕士研究生,主要研究方向为通信网络安全、移动通信技术(liushuxin11@gmail.com);彭建华(1966-),男,教授,硕士,主要研究方向为移动通信技术、无线通信安全;刘彩霞(1974-),女,副教授,博士,主要研究方向为电信网安全防护;谢晓龙(1974-),男,硕士研究生,主要研究方向为移动通信网安全.

应的字段(如中间人),对网络造成注册劫持、会话终止等威胁。

b)信息泄露。用户信息和拓扑信息伴随整个 SIP 协议消息的通信过程,信息存在泄露的可能性。



(a)注册流程



(b)基本会话流程

图2　SIP重要流程分析示意图

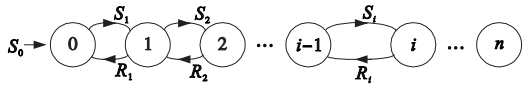


图3　流程实体收发链

针对以上问题,本文基于 Fuzz 测试设计了一种 SIP 流程漏洞挖掘模型,通过模拟 SIP 流程中实体的操作,对 SIP 流程进行漏洞挖掘。

如图 4 所示,模型包括检测设备和待检 IMS 网络。其中,检测设备包括三个功能:a)消息注入功能,确定实体 i,根据 i 产生相应的测试消息,发送到实体 i;b)监控功能,负责漏洞的判决,通过监控实体返回的消息,判定当前消息是否存在可能的安全漏洞;c)记录处理功能,记录存在漏洞的消息 S_i 及其响应结果。

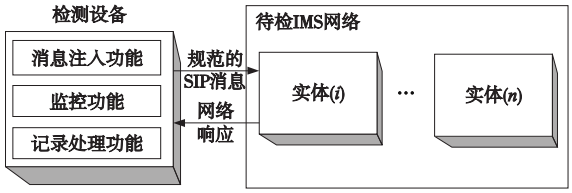


图4　IMS网络SIP漏洞挖掘模型

具体流程中,设 V_i 为节点 $i-1$ 对 S_{i-1} 消息字段的增删集合(参考 RFC-3261),流程节点间消息集合的关系如下:

$$S_1 = S_0 \cup V_1$$
$$S_2 = S_1 \cup V_2$$
$$\vdots$$
$$S_i = S_{i-1} \cup V_i$$

进一步推导:　$S_i = S_0 \cup V_1 \cup V_2 \cdots \cup V_i$　　(1)

因此,消息注入功能的实现可转换为初始消息 S_0 的生成。

模型中,节点 i 为待检网络的第一个实体。检测设备对接收到的消息 R_i 进行处理,其结果 $O_i = f(S_i, R_i)$。监控功能 f 负责判定结果 O_i 是否存在安全漏洞;最后记录处理功能记录 (S_i, R_i) 中的消息实例。

根据上述模型,设计总体漏洞挖掘流程如图 5 所示。首先产生测试消息并发送到实体 i;然后通过监控功能监控网络响应,判定其是否存在漏洞;最后对存在漏洞的消息进行记录处理,并跳转至开始重复执行。整个过程循环进行,挖掘 SIP 流程中不同 IMS 实体存在的安全漏洞。

消息注入功能和监控功能是模型的核心部分,在具体功能实现中,设计了相应的消息注入方法和监控方法,下文对其作进一步讨论。

2　功能实现

2.1　消息注入方法

随机消息产生是一般 Fuzz 测试消息产生的主要方法[9,10],但是在 IMS 网络实际的 SIP 注册流程中(register#1-401-register#2-200 OK),由于消息请求和响应之间的相关性,随机产生方法仅随机构造 register#1,并不能进入协议流程内部。同样,INVITE 消息也需要注册后才可以有效发送。

为了让产生的测试消息进入到 SIP 流程内部,以及保持流程间的随机性,本文结合 SIP 消息的基本流程和 Fuzz 测试的思想,设计了一种初始状态转移方法如图 6 所示。该方法利用随机过程状态空间转移的思想,在单一流程消息间,以响应消息为转移条件生成流程中下一个请求消息;在不同流程间,通过平均概率转移保持其随机性。具体注册流程中,把两个注册消息分类标记为 register#1 和 register#2,根据流程中返回消息响应 401 生成 register#2 消息,如图 6 中 REG#1 至 REG#2 的状态转移,转移条件为响应 401;在会话流程中,根据上一注册成功后的响应 200 OK,构造当前 INVITE 消息,如图中 REG#2 至 INVITE 的状态转移,转移条件为响应 200 OK;在其他消息生成中,通过以平均概率随机生成当前测试消息(图 6 中数字标注部分),达到不同流程中的随机切换。

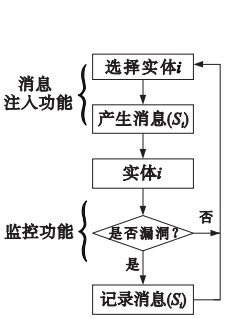


图5　模型总体流程

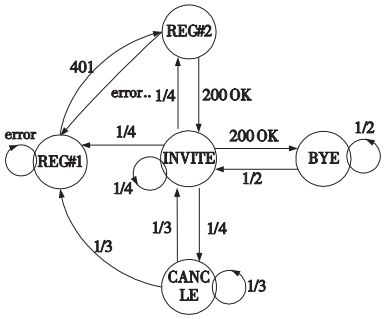


图6　初始消息状态转移图

初始消息状态转移方法的步骤如下:

a)随机选择待测实体 i,根据收到的响应 R_i,参照初始消息状态转移序列函数,选择当前 S_0 消息(初始为 register),若条件转移则实体 i 不变,否则随机生成实体 i。

b)根据协议规范随机生成 S_0 集合中的每一个消息字段值,S_0 构造完毕。

c)利用式(1)计算检测消息 S_i,并发送至实体 i。

d)响应 R_i 或超过等待时间 t_{out},跳转至步骤 a)。

2.2　监控方法

一般的监控方法主要以单一的软件崩溃或挂起作为标准[11,12],本文针对的对象是 SIP 流程,流程中存在的安全问题不同,需要监控的内容也不同,且其相应的监控方法各异。为了适应不同的监控内容和覆盖更多的安全漏洞,设计了一种自适应监控方法如图 7 所示。该方法可根据监控内容对返回的响应进行过滤,选择合适的方法进行监控。

具体步骤中首先开启监控计时,并接收消息响应;然后根

据监控内容选择相应的监控方法，如监控内容是崩溃挂起时，自动选择方法 1；最后利用选取的方法过滤并处理响应消息得出监控结果。在整个漏洞挖掘过程中，监控功能不断地选取适合监控内容的监控方法处理响应消息，相比单一监控（崩溃挂起）模型监控能够覆盖更多的安全漏洞。

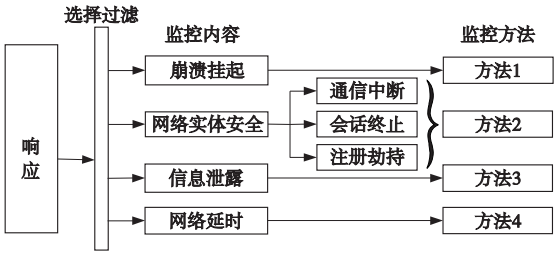


图7 自适应监控方法

具体针对性监控方法如下：

a）协议崩溃或挂起。从 t_{out} 开始计时，累积超过挂起时间 T_{out}（$T_{out} >> t_{out}$）作为软件挂起和崩溃的指标。

b）网络实体安全威胁的监控。针对可能产生通信中断、会话终止和注册劫持的情况监控，具体监控 SIP error（403、408、600 等）和 t_{out} 时间内非 SIP 消息。

c）信息泄露的监控。包含用户信息和网络拓扑信息，用户信息采取对定点的 SIP 字段（contact、authorization 等）作请求和应答对比，若存在两消息信息不同的情况，视为存在用户信息泄露的隐患。SIP 消息中含有大量的地址消息字段（path、route 等），其中包含大量的会话路由信息、网络拓扑信息和终端地址信息[13,14]。以 via 字段为例，通过提取 S_i 和 R_i 中的地址字段集合 S_{via} 和 R_{via}，并记录返回消息中多出的地址字段条数，即 $n_{via} = \text{num}\{R_{via} \setminus (S_{via} \cap R_{via})\}$ 判断其是否存在信息泄露的标准。消息流程中所有字段泄露为 $n = n_{via} + n_{route} + \cdots$，若判断 $n \geqslant n_a$，则存在泄露的可能。

d）网络延时监控。从起始发送消息开始计时，累积响应时间 $t \geqslant t_{delay}$（$t \leqslant t_{out}$，即在软件挂起范围外），则认为此时存在数据延迟的可能（通常情况下，也可以对数据包的数目进行分析），具体参数 t_{delay} 根据网络情况设置。

监控中可以根据不同的需求添加监控内容和方法，监控结束，对于可能存在安全隐患的测试消息，移交记录处理功能。

3 模型验证分析

利用 OpenIMSCore 开源仿真软件包搭建 IMS 网络环境，包括四个实体：HSS、P-CSCF、I-CSCF 和 S-CSCF，分别部署在四台 PC 终端上（系统为 Ubuntu 10.04.2，内存 1.00 GB，CPU 为 Pentium 3.20 GHz）。四台 PC 终端通过一个路由器互连组成简单的 IMS 网络，如图 8 所示。SIP 会话终端由 uctimsclient 1.0.13 软件实现，注册用户为 Bob。检测实体作为漏洞测试平台实现模型的消息注入、监控和记录处理功能。sip：alice@open-ims.test 为检测设备中发出的 SIP 消息 URI。

3.1 模型测试

本文对理论上存在的漏洞和实验结果进行对比，验证模型的有效性。实验过程中根据网络规模和测试效率，设置模型等待时间为 $t_{out} = 0.3$ s（为了提高 INVITE 消息的覆盖程度，每隔 1 s，正常注册一次），$T_{out} = 40$ s，$n_a = 1$。持续 15 min 后，检测设备记录处理功能中记录了可能出现安全漏洞的 SIP 消息，本文根据不同的监控内容，对模型的有效性进行详细分析。

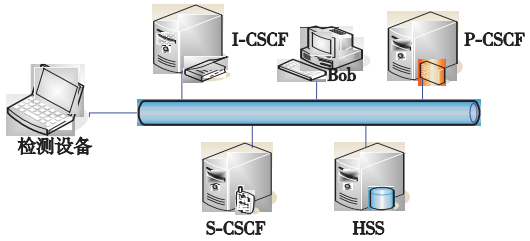


图8 IMS网络验证环境

1）字段修改监控 IMS 网络 SIP 流程中间节点存在恶意修改 SIP 头字段的威胁，为了验证模型对其进行漏洞挖掘的效果，以 register 消息中 max-forward 字段值修改后导致流程中断为例，对比了理论上消息字段修改和实验监控的结果。表 1 中结果显示了模型均能够检测消息修改威胁，具体结果也大致相同，说明模型能够对消息头字段修改导致的安全隐患作出相应的挖掘。其中，在 max-forward = 0 时，出现 483-too many hops，是由于消息发送中跳数 0 减 1 后，变量出现最大值导致出现 483-too many hops；最后一条中出现 600 busy，由于转发至 S-CSCF 时 max-forward = 0，该消息被丢弃掉，致使 I-CSCF 误判 S-CSCF 系统繁忙而产生 600 消息。总体看来，模型一定程度上能够挖掘字段修改导致的安全隐患。

表 1 max-forward 字段检测结果对比列表

消息类型	字段值	实体 i	理论结果	监控结果
register	max-forward:0	P/I/S-CSCF	无响应	483
register	max-forward:1	P-CSCF	无响应	无
register	max-forward:1	I-CSCF	注册超时	504
register	max-forward:2	P-CSCF	注册超时	504
register	max-forward:3/2	P/I-CSCF	注册超时	600

2）网络拓扑监控 信息泄露是 IMS 网络 SIP 流程的重要安全隐患之一，尤其是在 SIP 路由中拓扑信息的泄露。为了验证了模型对于拓扑信息泄露的挖掘效果，以 register 消息流程为例，对比了理论上的流程泄露拓扑信息和实验监控的结果。表 2 中显示了其实验结果对比，register 地址字段相对偏少，实验中设置的 $n_a = 1$，门限比较底，所以表中显示结果均能够检测出实体地址泄露。若 $n_a = 2$ 时，则部分拓扑泄露难以检测出来，可以根据检测的精度要求调节模型的门限值。

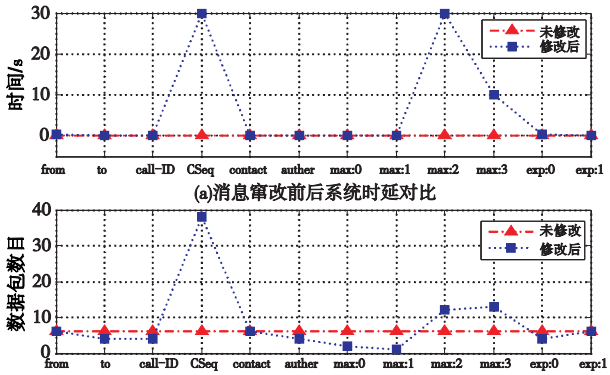
表 2 模型检测的 register 流程拓扑泄露漏洞

消息类型	实体 i	理论结果	实验监控结果
register	P-CSCF	P/S-CSCF 地址泄露	$n_{path} = 1$；$n_{service-route} = 1$；$n = 2 \geqslant 1$ 泄露
register	I-CSCF	S-CSCF 地址泄露	$n_{service-route} = 1$ $n = 1 \geqslant 1$ 泄露
register	S-CSCF	S-CSCF 地址泄露	$n_{service-route} = 1$；$n = 1 \geqslant 1$ 泄露

3）网络时延监控 本实验中以网络时延问题为监控内容，对 IMS 网络中消息字段修改对整个网络的危害及威胁程度作了进一步实验分析。在模型验证中发现，很多窜改后的消息占用了大量的网络资源。针对资源占用问题，通过发送到相同实体（P-CSCF）的 register 消息，对比其窜改前后系统产生的数据包数量和系统时延。

图 9（a）中显示了系统处理正常消息和修改后消息时延的对比情况。由于系统繁忙程度等的影响，每次正常 register 消

息响应时间并不完全相同,在(b)中则呈现了正常情况下产生的数据包和修改后系统产生数据包对比。通过对比可以看出,修改不同的字段对系统时延的影响并不相同,两图的总体走势大致相同,说明数据包的多少和系统时延是相关的。具体修改后的消息会对系统的性能产生一定的影响,尤其是修改 CSeq:1 INVITE、max-forward:3 等字段时,数据包数量分别为 38 和 13 个,其时延为 29.982 s 和 9.992 s,相比正常状态下的 register 的系统资源消耗(产生 6 个 SIP 数据包,平均时延 0.066 4 s)明显偏大(此时超出监控设置门限,判定为漏洞)。可以推断,如果发送大量上述类型的消息,将会比一般的 SIP 洪泛消息浪费更多的网络资源,进而产生 DoS 安全威胁。



(a)消息窜改前后系统时延对比

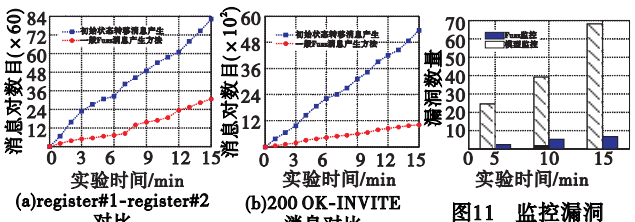
(b)消息窜改前后产生数据包数量对比

图9　消息窜改前后对比

3.2　模型功能测试

消息注入功能测试中,根据消息状态转移图,注册流程中 register#1-401-register#2-200 OK,若检测消息能够进入到消息流程内部,则需要连续发送 register#1 和 register#2。在会话流程中则是 200 OK-INVITE,本文以两种消息对的数目作为衡量检测消息进入流程内部的情况。图 10 显示了随机消息产生和初始消息状态转移方法中,register#1-register#2 和 200 OK-INVITE 消息对数目的变化,模型产生的消息对数较多,说明模型初始消息状态转移方法能够使检测消息深入到流程内部。但在资源耗费上,检测设备运行初始消息状态转移方法在 CPU 使用率(约为 67%)上相比随机产生方法(约为 52%)偏高。

针对监控功能,图 11 显示了自适应监控方法和单一监控方法(崩溃挂起)中漏洞数量的对比。图中显示两者数量差距较大,其中由于能够同时监控拓扑信息泄露现象和字段修改等多种监控内容,并实施相应的监控方法,所以模型中监控到的漏洞数量较多。



(a)register#1-register#2 对比

(b)200 OK-INVITE 消息对比

图10　流程检测消息对比

图11　监控漏洞数量对比

4　结束语

针对 IMS 网络 SIP 流程中存在的安全漏洞,本文在 Fuzz 测试的基础上,建立了漏洞挖掘模型。在消息注入功能实现中,针对 SIP 流程特点,提出初始状态转移方法,使检测消息进入流程内部,并实现了自适应监控功能。模型检验中,搭建了 IMS 网络环境对提出的模型进行检验,检验结果对比表明,该模型初始消息转移方法能够深入到流程内部,自适应监控方法能够覆盖更多的安全漏洞。本文在拓扑泄露监控中只是检测是否存在漏洞,缺少具体细节,下一步研究将针对不同 SIP 字段拓扑泄露程度作量化估计。

参考文献:

[1] 王尚广,孙其博, 杨放春. IMS 网络中的 SIP 洪泛攻击检测[J]. 软件学报,2011,22(4):761-772.

[2] KUMAR A,TILAGAM S. A novel approach for evaluating and detecting low rate SIP flooding attack[J]. International Journal of Computer Application,2011,26(1):31-36.

[3] CHEN E Y,ITOH M. A whitelist approach to protect SIP servers from flooding attacks[C]//Proc of IEEE International Workshop Technical Committee on Communications Quality and Reliability. 2010:1-6.

[4] SCHANES C,TABER S,POPP K,*et al*. Security test approach for automated detection of vulnerabilities of SIP-based VoIP softphones[J]. International Journal on Advances in Security,2011,4(1-2):95-105.

[5] CHOWOHURY M Z,SY B K,AHMAD R. Application of gassian estimation for devising reliable vulnerability assessment on SIP-based VOIP infrastructure[C]//Proc of International Conference on Security & Management. 2006: 293-299.

[6] GORBUNOU S,ROSENBLOOM A. AutoFuzz:automated network protocol fuzzing framework[J]. International Journal of Computer Science and Network Security,2010,10(8):239-245.

[7] CAMARILLO G, GARCIA-MARTIN M A. The 3G IP multimedia subsystem (IMS):merging the internet and the cellular worlds[M]. 2nd ed. Chichester: John Wiley,2006:31-40.

[8] SHUANG Kai,WANG Si-yuan,ZHANG Bo,*et al*. IMS security analysis using multi-atttibute model[J]. Journal of Networks,2011,6(2):263-271.

[9] BECKER S, ABDELNUR H, OBES J L, *et al*. Improving fuzz testing using game theory[C]//Proc of the 4th International Conference on Network and System Security, Melbourne, Australia. Washington DC: IEEE Computer Society,2010:263-268.

[10] DAI Hu-ning, MURPHY C, KAISER G E. Configuration fuzzing for software vulnerability detection[C]//Proc of International Conference on Availability, Reliability and Security. 2010:525-530.

[11] TAKANEN A, DeMOTT J, MILLER C. Fuzzing for software security testing and quality assurance[M]. Norwood, MA: Artech House, 2008:22-32.

[12] WANG Tie-lei,WEI Tao,GU Guo-fei,*et al*. TaintScope: a checksum-aware directed fuzzing tool for automatic software vulnerability detection[C]//Proc of IEEE Symposium on Security and Privacy. 2010: 497-512.

[13] JACOB C,PFEFFER H, LINNER D,*et al*. Automatic routing of semantic SIP messages in IMS[C]//Proc of the 2nd International Conference on Internet Multimedia Services Architecture and Applications. 2008:1-6.

[14] GURBANI V K, CHIANG T C, KUMAR S. SIP: a routing protocol [J]. Bell Labs Technical Journal,2001,6(2):136-152.