Journal of Wuhan Polytechnic

基于 SIP 的 VoIP 软终端自动测试方法

叶自宁

(武汉职业技术学院,湖北 武汉 430074)

摘 要: VoIP 系统已经成为商业应用中重要的一部分,为了促进 VoIP 应用的健壮性发展,需要一种可以有效检测其安全漏洞的自动安全测试工具。本文提出了一种基于模糊测试的框架,用于检测基于 SIP 的 VoIP 软电话安全漏洞。该框架可以自动与软电话用户界面进行交互,并且可以观察软电话的用户界面来检测错误信息。实验证明提出的框架可以检测出以前没有发现的一些漏洞。

关键词: SIP;VoIP;自动测试;用户图形界面;模糊测试

中图分类号: TP27 **文献标识码:** A **文章编号:** 1671-931X (2011) 05-0066-04

引言

会话初始协议(Session Initiation Protocol,SIP)[1]是由 IETF 提出的,用于控制会话通信的协议。SIP 是基于明文的,定义了两种通信成员:User Agent(UA)和服务器。UA 用于初始或结束会话的软终端或电话。服务器对 UA 提供服务,例如注册或中转呼叫等。

SIP 协议广泛应用于 VoIP 系统中,通信中一方的软终端可以与另一方软终端建立呼叫,因此攻击者可以远程引发 VoIP 电话中的漏洞。本文提出的框架是基于模糊测试的用于检测 SIP 软终端的漏洞。模糊测试是通过注入错误信息来进行漏洞检测的动态方法,最早由 Miller 等人提出用于检测应用中的安全漏洞[2],并广泛应用于多种应用软件的检测中[3][4]。本文关注对基于 SIP 的有用户图形界面的 UA 进行模糊测试。

破坏 SIP 中 VoIP 系统健壮性的消息可以归结为五种:错误的文法;域值越界;无效消息或域名;头字段的重复;无效语义[5]。本文的模糊测试框架支持这些规则产生的 SIP 数据,使用智能的基于模板的随机消息产生方法[6],引入状态机来测试 SIP 软终端的不同状态。使用 GUI 事件引擎自动触发测试系统(system under test,SUT)检测 SIP 的软终端,为了提高检测准确性,在客户端使用 GUI 检测器检测错误的会话和终端主机上程序窗口的改变。所提出的测试框架可以检测 VoIP 软电话漏洞,提高软终端健壮性。

一、相关工作

模糊测试是检测应用程序漏洞的技术[2],可以应用于 VoIP 中[6][7]。SIP 安全测试有很多工具,例如 PROTOS 测试套件[8]有大约 4527 个畸形消息来检测SIP 产品的健壮性。但不可以对 SIP 状态进行检测,例如 Calling 或 Ringing 等。

Banks 等人提出的 SNOOZE 测试框架[9]使用用户预先定义的场景,目前只能产生少量的畸形消息。另一个有状态的模糊测试是由 Abdelnur 等人提出的 KiF[10],使用 ABNF 文法描述消息语法,可以通过定义的规则自动产生畸形消息对不同状态进行测试并追踪状态信息。缺点是只通过对 SIP 响应分析测试结果,并且不能针对未定义的状态进行测试。

Alrahem 等人提出的 INTERSTATE[11]可以与软终端的 GUI 进行交互、自动接受呼叫等。测试中工具可以发送一系列 SIP 消息流程和 GUI 事件给 SUT,但是只对

收稿日期:2011-08-15

基金项目: 湖北省高等学校省级教学研究项目“基于高职网络教学评价策略的《组网与网络管理》课程网站研究与实现”(项目编号:2009SJ236)。

作者简介:叶自宁(1977-),男,湖北武汉人,硕士,武汉职业技术学院讲师,研究方向:信息管理、网络技术。

响应分析得到检测结果且不能监控软终端的 GUI 变化。

白盒模糊测试方法必须了解一些事先的内部信息，而很多软终端的代码不是开源的，所以我们使用黑盒测试方法。单纯的对响应进行分析并不能检测出某些潜在的漏洞，同时由于 GUI 在 UA 中的使用很多漏洞只有通过对 GUI 监控才能检测出来。所以我们结合了自动 GUI 交互方法，同时观察 GUI 行为综合搜集到的信息对测试结果进行分析，减少错报率。

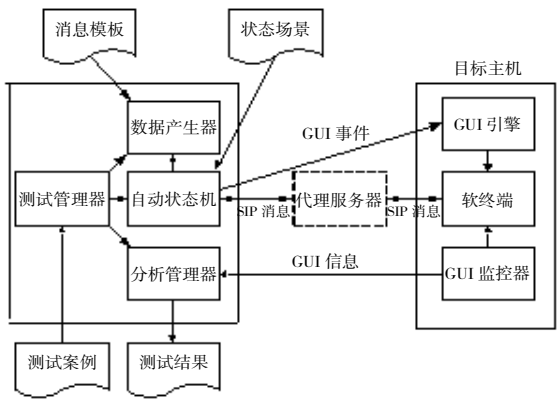

图 1 测试框架

二、测试工具的体系结构

本文实现的模糊测试工具使用的是通用的框架，可以用于不同应用程序的漏洞检测。测试 SIP 软终端时，使用基于模板的消息产生方法，包含了一个可以配置的 SIP 状态机用于 SIP 软终端的状态测试，如图 1 所示。测试工具使用 GUI 参与器和 GUI 监控器对 SUT 自动控制和监控。状态机通过控制测试主机中的 GUI 引擎触发软终端的 GUI 事件，GUI 监控器提供界面信息给分析器，综合这些信息决定测试结果。

SIP 可以在两个 UA 间直接建立连接，也可以通过代理服务器进行会话，本框架支持这两种方式。

（一）框架体系结构

框架的主要部分是测试管理器，用于控制测试执行，读取测试案例；数据产生器根据预先定义的消息模板流程等信息产生发送的消息；自动状态机包含 SIP 的状态和与 SUT 的 GUI 交互接口的实现；分析管理器集合了多种分析器，根据所控制的分析器得到的信息创建最后的测试结果存储到测试结果文件中。

数据产生器由自动状态机控制，负责消息的产生，包括正确的消息和畸形的消息。状态机的信息可以用来产生消息的不同部分，例如 ID 等。

自动状态机可以直接与 SUT 建立连接也可以通过代理与 SUT 建立连接，发送产生的 SIP 消息并接收响应。自动状态机允许用户定义状态机转换关系，配置任意状态。此外还支持无效的状态转换测试，通过使用未定义的状态转换测试 SUT 行为。每个状态都通过 GUI 事件使用 GUI 引擎和软终端 GUI 交互，测试案例的状态转换配置信息和 GUI 交互称为状态场景。自动状态机控制 SIP 软终端状态，将 SIP 软终端转换到一个需要测试的状态。

分析管理器包含几个不同种类的分析器：针对日志文件的分析器；针对响应的分析器；针对 SUT 中 GUI 的分析器；针对主机端口监控的分析器。不同分析器的使用提高了检测的准确率。

（二）与 SUT 的交互和监控

该框架允许定义 SIP 消息流程和 GUI 事件，用于远程的 SUT，GUI 事件的应用可以实现自动测试软终端的所有状态。SUT 主机的测试环境包括三个组成：软终端（SUT）、GUI 引擎和 GUI 监控器，如图 1 所示。

GUI 引擎是一个 JAVA 工具，使用 java.awt.Robot 执行 SUT 中的 GUI 事件与 GUI 元素交互。工具使用状态场景中的 GUI 事件文件与 GUI 参与器通信，GUI 事件文件是一系列的 GUI 事件。GUI 参与器的使用可以自动对 SUT 执行测试。

应用中的错误信息可以在不同的 GUI 元素显示，例如会话中通过 xwininfo 实现 GUI 监控器原型，GUI 监控器分析 xwininfo 并存储这些信息在一个树结构中。测试案例要存储这些信息，GUI 监控器使用这些信息检测窗口的改变决定测试的结果。

三、测试框架实现的案例

工具提供不同测试场景配置测试 SIP 软终端，每个场景是一个单独的案例。目前版本可以实现 4 种不同的场景来验证 GUI 交互和监控 GUI 的运行。

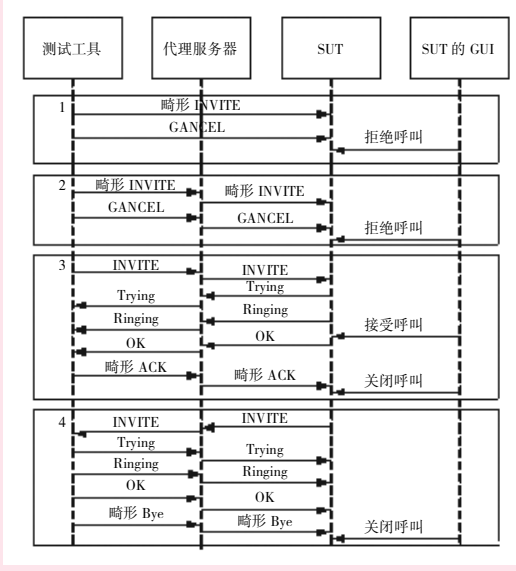

图 2 测试场景

如图 2 为目前版本的主要测试场景配置。第一个场景工具发送畸形 INVITE 消息直接给 SUT，是无状态的测试。DoS 攻击是基于该场景的，不需要附加的条件和消息发送给 SUT。第二个场景与第一个类似，工具通过代理发送畸形的 INVITE 消息给 SUT。第三个场景由工具发起的呼叫，通过代理发送一个畸形的 ACK 消息给 SUT。第四个场景中 SUT 初始呼叫，工具回应有效的 Trying、Ring 和 OK 消息，工具不等待 SUT 端的 ACK 消

息直接发送一个畸形的 Bye 消息，会话结束。第三、四个场景中，SUT 中的 GUI 需要参与其中来进行自动的测试，SUT 可以发起或接受呼叫。

根据预先定义的规则产生多种不同的 SIP 消息应用在不同的测试案例中。消息的产生和案例的处理是基于模板文件的，模板中包含占位符和配置信息。每个占位符是一个单独的测试案例，只有当前测试案例中的占位符会有特定值，其他占位符需要时可以被一些静态信息或随机产生的数据替代。

测试架构允许使用附加信息对特殊值进行测试。测试案例使用随机修改 SIP 头域顺序的方法对不同头域值或重复头域值进行测试。

测试框架使用分析器决定测试结果，多种不同的分析器用来分析软终端不同的漏洞。例如使用一种分析器专门查看 SUT 接收的响应是否包含特定的关键字，Exception 或 Error。另一种分析器通过监控 SUT 端口查看应用是否有效。

还可以使用分析器对 SUT 日志文件进行关键字查找，或对 SUT 的 GUI 进行监控。分析器通过案例执行前后主机 GUI 窗口对比判断 GUI 是否改变。对于最近打开和关闭的窗口，分析器通过名字得到与 SUT 窗口的关系。SIP 软终端窗口的关系和主机其它应用窗口的关系是不同的，可以通过 SUT 主机上运行的 GUI 分析器了解软终端的状态信息。

四、实验结论

实验使用 Asterisk 作为代理服务器，测试中使用两个不同的账户，其中一个作为 SIP 软终端(SUT)另一个为测试框架。测试案例使用 Asterisk 作为注册和代理服务器，所有的消息都经过它发送。

使用该模糊测试框架对两款 SIP 软终端进行测试，测试场景为第 3 部分提到的测试场景，每个场景都可以检测到一些未知漏洞，包括 DoS、内存耗尽和 Cross Site Scripting(XSS)漏洞。

测试执行结果证明每个分析器都有各自的缺点和优点，但是每个分析器都可以查找出不同的漏洞，因此使用它们可以降低错报率。

(一)测试 SIP 软终端

测试两种不同的软终端。第一种测试目标 QuteCom 是用 Python、C 和 C++ 编写的开源 SIP 产品，测试版本是 2.2 revg-20100116203101。第二种软终端是 SIP Communicator，使用 JAVA 编写的开源 VoIP 客户端，测试版本是 1.0-alpha3-nightly.build.2351。

两种软终端都可以在 Windows 和 Unix 平台运行，测试的主机系统上运行 Linux Ubuntu。不使用 GUI 监控器的情况下可以发现 QuteCom 在 Windows 下不能检查 SIP 头域的内容长度。每次内容长度小于真实长度时软件会发生崩溃。最新版本的 QuteCom 已经修复了这个漏洞。

(二)详细测试结果

本文提出的自动测试框架可以检测出两种软终端的漏洞，例如 SIP Communicator 的 DoS 漏洞。SIP Communicator 使用固定源端口，范围从 5000 到 6000 且不能复用，当这 1000 个端口被占用后，就不能处理其余呼叫。该漏洞是 GUI 分析器检测出来的。SIP Communicator 在日志文件监控中检测到一个问题，java.lang.NullPointerException。该漏洞不能通过 GUI 监控器检测出来，因为 GUI 不能显示出这样的错误信息。测试框架可以识别出来 XSS 漏洞，因为 SIP Communicator 使用 javax.swing.JoptionPane 重组错误的会话，使用 javax.swing.Jlabel 递交文本。发送给 SUT 一个包含 HTML 代码注入的 SIP 请求引发漏洞。

QuteCom 同样有 DoS 漏洞，工具使用 GUI 引擎触发 SUT 中的结束按钮点击事件，导致应用崩溃。该漏洞通过 GUI 分析器和端口分析器检测到。QuteCom 中的内存耗尽漏洞是通过并行呼叫在 Ringing 状态检测到的，关闭 Ringing 状态的会话导致应用崩溃。通过 SUT 的端口监控器检测到了这个崩溃。这说明今后的测试需要定义附加并行交互测试场景信息。

(三)结论

使用不同的分析器检测不同的漏洞。分析结果的正确率根据不同标准有所不同。监控端口检测具有比较高的正确率，只当网络出现问题才会造成错报，例如防火墙阻止了某个需要测试的端口。基于关键字分析响应可以判断响应是否包含一些错误信息，使用这些信息来进行自动测试更多的依赖于错误处理的具体实现。很多漏洞只能通过 GUI 行为分析器检测到，不同分析管理器中的分析器降低了错报率。

五、总结

本文提出了一种自动安全测试的方法，通过 GUI 的使用检测漏洞增强了 VoIP 服务通信的安全性。该检测方法通过发送 SIP 消息和 GUI 引擎控制软终端来自动检测 SIP 的不同状态。多个分析器结合自动检测 VoIP 软终端安全漏洞，例如 SUT 响应和端口分析器。

使用本文的测试框架对两种开源的 SIP 软终端进行测试，实验证明可以检测出多个安全漏洞，例如 DoS 和内存耗尽等。其中多个漏洞是对 SUT 的 GUI 监控检测到的，这说明 GUI 监控对安全测试是十分必要的。

参考文献：

[1] J.Rosenberg, H.Schulzrinne, G.Camarillo.SIP: Session Initiation Protocol[S].IETF, 2002.

[2] J.E.Forrester, B.P.Miller.An empirical study of the robustness of Windows NT applications using random testing: Proceedings of the 4th conference on USENIX Windows Systems Symposium [C]. Berkeley CA, USA:USENIX Association, 2000:6-10.

[3] V.Ganesh, T.Leek, M.Rinard.Taint-based directed whitebox fuzzing :IEEE 31st International Conference on Software Engineering[C]2009:474, 484.

[4] E.Y.Chen, M.Itoh.Scalable detection of SIP fuzzing attacks: Second International Conference on Emerging Security Information Systems and Technologies.SECURWARE, 2008:114, 119.

[5] P.Oehlert.Violating assumptions with fuzzing[J],Security &Privacy, IEEE.2005,(3):58,62.
[6] Li Hongbin,Lei Weimin,Yang Xuehua.SIP-based research in VoIP security testing tools.Jounal of Chinese Computer System,2010,31(10):2017-2023.
[7] H.J.Abdelnur,R.State,O.Festor.KiF: a stateful SIP fuzzer: Proceedings of the 1st international conference on Principles, systems and applications of IP telecommunications [C]. New York, NY, USA: ACM, 2007:47,56.
[8] U.Oulu.PROTOS:Security testing of protcol implementations [EB/OL].2010-02-14.https://www.ee.oulu.fi/research/ouspg/Protos.
[9] G.Banks,M.Cova,V.Felmetsger,et al.SNOOZE:toward a stateful Network protocol fuzzer:Proc of the 9th International Conference on Information Security[C].2006:343-358.
[10] H.J.Abdelnur,R.State,O.Festor.Advanced fuzzing in the VoIP space[J],Journal in Computer Virology, 2010,(6):57 64.
[11] T.Alrahem,A.Chen,N.DiGiussepe,J. Gee, S.-P. Hsiao, S. Mattox, T. Park, A. Tam, and I. G. Harris, "INTERSTATE: A stateful protocol fuzzer for SIP," 2007.

[责任编辑：刘 骋]

Automatic Security Test Approach for SIP-based VoIP Softphones

YE Zi-ning
(Wuhan Polytechnic, Wuhan430074, China)

Abstract: VoIP systems have become an important part in business applications. In order to ensure the safety of VoIP, we need a security test tool which can test the vulnerabilities of SIP applications automatically. This paper presents a framework of the fuzzy test to detect the vulnerabilities of SIP-based softphones. The presented approach automates the interaction with Graphical User Interface of softphones during testing and can detect application errors by monitoring the softphone graphical user interfaces automatically. The results show that the framework is capable of detecting the flaw.

Key words: SIP ; VoIP; automatic test; graphical user interface; fuzzy test

（上接第 57 页）

企业强强联合，优势互补。要发挥关联性大、带动性强的大企业集团的示范、辐射、信息扩散和营销网络的产业龙头作用，实现社会资源向龙头企业聚拢，并联合中小企业分工协作，拧成一股绳共谋产业集群品牌的发展。

参考文献：

[1] 王敏.博弈论视阈下的企业品牌战略研究[J].经济视角，2009,(10).
[2] 宜昌市政府工业经济结构调整问题研究课题组.宜昌市工业经济结构调整问题研究[J].三峡论坛,2010,(5).
[3] 潘天群.博弈思维——逻辑使你决策制胜[M]. 北京：北京大学出版社,2005.
[4] George A.Akerlof. The market for lemons:quality uncertainty and the market mechanism [J].The Quarterly Journal of Economics, 1970, (3).

[责任编辑：张 磊]

Study on Development Strategies of Regional Industrial Cluster Brand from the Perspective of Game Theory ——A Case Study of Equipment Manufacturing in Yichang City, Hubei Province

QI Long-qi
(Hubei Three Gorges Polytechnic, Yichang443000, China)

Abstract: Industrial cluster brand has been the result of economic development, which arouses more and more concerns. Based on game theory, the article examines the development of equipment manufacturing clusters brand at present, identifies the problems arising, and puts forward seven constructive development strategies.

Key words: industrial cluster brand; equipment manufacturing; Game Theory; Yichang city