(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104796240 B
(45)授权公告日 2018.06.05

(21)申请号 201510219969.2

(22)申请日 2015.04.30

(65)同一申请的已公布的文献号
申请公布号 CN 104796240 A

(43)申请公布日 2015.07.22

(73)专利权人 北京理工大学
地址 100081 北京市海淀区中关村南大街5号

(72)发明人 胡昌振 马锐 郭林楠 单纯 王达光

(74)专利代理机构 北京理工大学专利中心 11120
代理人 高燕燕

(51)Int.Cl.
H04L 1/24(2006.01)

(56)对比文件
CN 102087631 A,2011.06.08,
CN 104142888 A,2014.11.12,
US 7310606 B2,2007.12.18,

审查员 许顺频

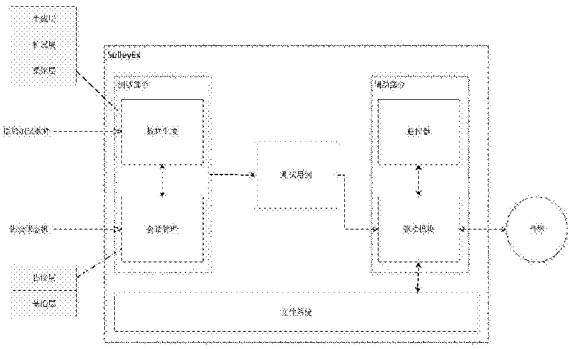
权利要求书1页 说明书4页 附图3页

(54)发明名称

一种有状态网络协议的模糊测试系统

(57)摘要

本发明提供一种有状态网络协议的模糊测试系统，解决了传统网络协议模糊测试框架缺乏对复杂的、有状态协议的支持问题。包括数据生成模块、会话管理模块、监控器、驱动模块；其中：数据生成模块用于存储原始数据样本，并基于规则树算法对原始数据进行模糊化，生成模糊测试用例；会话管理模块用于将模糊测试用例中定义的一个或多个请求连接为一个有向无环图，然后针对每一条路径进行模糊测试；监控器包括进程监控器与网络监控器；驱动模块用于与待测目标服务器通信，发送测试请求并接收服务器响应消息。



CN 104796240 B

1.一种有状态网络协议的模糊测试系统，其特征在于，包括数据生成模块、会话管理模块、监控器、驱动模块；其中：

数据生成模块用于存储原始数据样本，并基于规则树算法对原始数据进行模糊化，生成模糊测试用例；数据生成模块首先取得原始数据样本，然后根据协议请求格式将其表示成为一个请求；

会话管理模块分为基础层和协议层两层；基础层为基础的会话类；协议层针对不同的协议定义相应的状态机，并根据状态机生成相应的会话过程；会话管理模块用于将模糊测试用例中定义的一个或多个请求连接为一个有向无环图，每一个图有至少一个起点，每个节点代表一个请求，分支表示一个请求之后有多种可能的后续请求，一条路径即是一次模糊测试过程；将一个复杂协议分解为多个单独的请求过程，同时利用相应协议的有限状态机的转换图，生成该协议所有的状态转换路径，然后针对每一条路径进行模糊测试；

监控器包括进程监控器与网络监控器；进程监控器用来检测待测程序进行是否出现错误，如果模糊测试用例引发进程出现异常或崩溃，则进程监控器发出异常提示消息；网络监视器负责监控网络通信，并把通信过程记录在相应的文件中，方便检查错误；

驱动模块用于与待测目标服务器通信，发送测试请求并接收服务器响应消息。

2.如权利要求1所述的一种有状态网络协议的模糊测试系统，其特征在于，其中所述的一个请求是一次状态转换测试中的一个数据单元，其中包括多个数据原子，或其他复杂的数据结构；一个或多个请求的有序组织即组成模糊测试的一个测试用例。

3.如权利要求1或2所述的一种有状态网络协议的模糊测试系统，其特征在于，其中所述的数据生成模块分为三层，分别为原始层、扩展层和生成层；原始层为原始数据类型，包括整数、浮点数、字符基本数据类型；扩展层在原始层提供的基础数据类型进行整合，同时为不同协议提供不同的数据块结构，方便用户定义原始数据；生成层利用基于状态机的网络协议半合法化的模糊测试用例生成算法生成测试用例，该算法根据网络协议规约，提取网络协议相关信息并解析协议格式，构建网络协议状态机以及基于有限状态机的网络协议规则树，同时利用对状态转换路径的标记来缩小模糊测试用例规模。

4.如权利要求1或2所述的一种有状态网络协议的模糊测试系统，其特征在于，其中所述的监控器分为进程监控器、网络监控器、虚拟机控制器三个监控工具，与待测程序运行在同一台计算机上，称为被测机。

一种有状态网络协议的模糊测试系统

技术领域

[0001] 本发明涉及一种有状态网络协议的模糊测试系统，属于模糊测试领域。

背景技术

[0002] 术语解释：

[0003] 模糊测试：模糊测试是黑盒测试的一种具体技术，在安全性测试中越来越受到重视。它的原理是将大量的畸形数据输入到目标程序中，通过监测被测程序的异常来发现被测程序中可能存在的安全漏洞。它是一个典型的自动或半自动的过程。

[0004] 网络协议模糊测试：网络协议是指计算机网络中互相通信的对等实体间交换信息时所必须遵守的规则的集合。在网络协议模糊测试中要求识别攻击的界面，变异或生成包含错误的模糊值，然后将这些模糊值传递给一个目标应用，并监视目标应用以发现错误。

[0005] 有状态网络协议：服务器在接收到客户端的请求后，会返回对应的响应，协议的状态是指下一次请求响应的时候会受本次请求的影响。有状态网络协议即要求服务器可以记录响应后的状态，并可恢复此次状态。

[0006] 模糊测试框架：模糊测试框架是可以用于不同类型目标进行模糊测试的工具，它简化了许多种不同类型的测试目标的数据表示方法。标准的模糊测试框架一般包含测试用例生成、网络和磁盘传输以及脚本类语言三部分。

[0007] 模糊测试是一种发现安全漏洞的有效的测试方法，在安全性测试中越来越受到重视。它的原理是将大量的畸形数据输入到目标程序中，通过监测程序的异常来发现被测程序中可能存在的安全漏洞。模糊测试中的网络协议测试是安全研究者来最感兴趣的部分，不仅因为所发现的漏洞通常具有较高级别的危险程度，而且还由于网络协议在互联网通信中被广泛应用，一旦被发现存在漏洞，受威胁的范围将会很广。

[0008] 模糊测试和其他的软件测试相比，体现其核心价值之处在于能够将大量的手工测试转化为自动化测试。生成单个测试用例是费力和枯燥的，而其中的某些部分则非常适合于让计算机来自动生成。模糊器的核心竞争力就是它能够在最少人工干预的情况下，自动化生成有用测试数据的能力。

[0009] 模糊测试框架是可以用于不同类型目标进行模糊测试的工具，它简化了许多种不同类型的测试目标的数据表示方法。标准的模糊测试框架包括三个部分：一个能够引发漏洞的方法库用来生成模糊测试用例；一系列例程用来简化磁盘输入输出和网络传输。现在已经有一些成熟的模糊测试框架，如SPIKE、Peach、 antiparser、Dfuz等，但目前这些框架都有着明显的缺陷，如SPIKE仅适用于 Linux系统，缺乏对Windows平台的支持，Peach对应用场景的描述要求则过于严苛与繁琐，antiparser只能做些简单的模糊测试，对于复杂情形则无法处理， Dfuz同样缺乏对Windows平台的支持，同时还不具备智能性。同时这些框架无法测试有状态协议的状态转换过程，如图1，只能分别测试A、B、C、D状态，但是无法对A-B-C或A-C-D进行处理。即现有针对网络协议的模糊测试框架，虽然能够发现协议实现中的漏洞，但是他们缺乏对复杂、有状态协议的支持，他们的测试脚本不能包含消息序列的整个状

态序列，并且协议模糊测试的覆盖范围不够完整。

发明内容

[0010] 本发明提供一种有状态网络协议的模糊测试系统，解决了传统网络协议模糊测试框架缺乏对复杂的、有状态协议的支持问题，以及传统网络协议模糊测试框架生成的测试脚本不能包含消息序列的整个状态序列，协议模糊测试的覆盖范围不够完整的问题。

[0011] 本发明通过以下技术方案实现：

[0012] 一种有状态网络协议的模糊测试系统，包括数据生成模块、会话管理模块、监控器、驱动模块；其中：

[0013] 数据生成模块用于存储原始数据样本，并基于规则树算法对原始数据进行模糊化，生成模糊测试用例；数据生成模块首先取得原始数据样本，然后根据协议请求格式将其表示成为一个请求；

[0014] 会话管理模块用于将模糊测试用例中定义的一个或多个请求连接为一个有向无环图，每一个图有至少一个起点，每个节点代表一个请求，分支表示一个请求之后有多种可能的后续请求，一条路径即是一次模糊测试过程；将一个复杂协议分解为多个单独的请求过程，同时利用相应协议的有限状态机的转换图，生成该协议所有的状态转换路径，然后针对每一条路径进行模糊测试；

[0015] 监控器包括进程监控器与网络监控器；进程监控器用来检测待测程序进行是否出现错误，如果模糊测试用例引发进程出现异常或崩溃，则进程监控器发出异常提示消息；网络监视器负责监控网络通信，并把通信过程记录在相应的文件中，方便检查错误；

[0016] 驱动模块用于与待测目标服务器通信，发送测试请求并接收服务器响应消息。

[0017] 其中所述的一个请求是一次状态转换测试中的一个数据单元，其中包括多个数据原子，或其他复杂的数据结构；一个或多个请求的有序组织即组成模糊测试的一个测试用例。

[0018] 其中所述的数据生成模块分为三层，分别为原始层、扩展层和生成层；原始层为原始数据类型，包括整数、浮点数、字符基本数据类型；扩展层在原始层提供的基础数据类型进行整合，同时为不同协议提供不同的数据块结构，方便用户定义原始数据；生成层利用基于状态机的网络协议半合法化的模糊测试用例生成算法生成测试用例，该算法根据网络协议规约，提取网络协议相关信息并解析协议格式，构建网络协议状态机以及基于有限状态机的网络协议规则树，同时利用对状态转换路径的标记来缩小模糊测试用例规模。

[0019] 其中所述的会话管理模块分为基础层和协议层两层；基础层为基础的会话类；协议层针对不同的协议定义相应的状态机，并根据状态机生成相应的会话过程。

[0020] 其中所述的监控器分为进程监控器、网络监控器、虚拟机控制器三个监控工具，与待测程序运行在同一台计算机上，称为被测机。

[0021] 本发明的有益效果：

[0022] 本发明中分为数据生成、会话管理、驱动、监控器等4个模块。其中，数据生成模块根据不同的协议定义了不同的数据块，同时将一种基于规则树的算法对原始数据进行模糊化，简化框架用户者的操作；会话管理管理模块将不同协议的状态机进行封装，从而解决了传统框架对协议状态转换过程中测试不充分的问题，同时也使本发明可适用于不同多种协

议。

附图说明

[0023] 图1为背景技术中状态转换路径示意图；

[0024] 图2本发明一种有状态网络协议的模糊测试系统结构框图；

[0025] 图3为本发明数据生成模块结构框图；

[0026] 图4为本发明会话管理模块结构框图；

[0027] 图5为本发明具体实施例中协议状态转换示意图；

[0028] 图6为本发明具体实施例中会话过程示意图；

[0029] 图7为本发明监控器模块结构框图。

具体实施方式

[0030] 下面举例一种基于有限状态机的网络协议模糊测试框架SulleyEX来对本发明作详细的介绍。

[0031] SulleyEX针对现有工具对有状态协议状态转换测试的不足，并根据有状态网络协议的特点，提出一种基于有限状态机的模糊测试框架。SulleyEX主要分为测试和辅助两部分，测试部分主要由数据生成模块和会话管理模块组成，辅助部分主要由监控器和驱动模块组成，如图 2 。

[0032] 1.数据生成模块

[0033] 数据生成模块是存储原始数据样本，并基于一种基于规则树算法对原始数据进行模糊化，并生成模糊测试用例。数据生成模块首先要取得原始数据样本，然后根据协议请求格式将其表示成为一个请求。一个请求是一次状态转换测试中的一个数据单元，其中可包括多个数据原子，如整数、浮点数、字符串等，也可能包括复杂的数据结构、如数据块、数据组等。一个或多个请求的有序组织即组成模糊测试的一个测试用例。(如图3)。

[0034] 数据生成模块分为三层，分别为原始层、扩展层和生成层。原始层为原始数据类型，包括整数、浮点数、字符等基本数据类型。扩展层是在原始层提供的基础数据类型进行整合，同时为不同协议提供不同的数据块结构，方便用户定义原始数据，该结构类似于面向对象语言中的结构类型。数据块结构以 s_block_start()开始，以s_block_end()结束。

[0035] 生成层利用基于状态机的网络协议半合法化的模糊测试用例生成算法生成测试用例，该算法根据网络协议规约，提取网络协议相关信息并解析协议格式，构建网络协议状态机以及基于有限状态机的网络协议规则树，同时利用对状态转换路径的标记来缩小模糊测试用例规模。

[0036] 2.会话管理模块

[0037] 会话管理模块的工作是将测试用例中定义的一个或多个请求连接为一个有向无环图，每一个图有至少一个起点，图中每个节点代表一个请求，图中的分支表示一个请求之后有多种可能的后续请求。图中的一条路径即是一次模糊测试过程。这样的方法可以将一个复杂协议分解为多个单独的请求过程，同时利用相应协议的有限状态机的转换图，可生成该协议所有的状态转换路径，然后针对每一条路径进行模糊测试。通过这样的方法即可完整覆盖所有路径，提供了完整的测试覆盖率。(如图4)

[0038] 会话管理模块分为基础层和协议层两层。基础层为一些基础的会话类，如与服务器连接的connection类，描述测试目标的target类，处理异常的handler 类等。协议层中针对不同的协议定义的了相应的状态机，如SMTP、SIP、FTP协议等，并根据状态机生成相应的会话过程。假设某有状态协议状态转换过程如图 5 。选取其中一条状态转换路径，如S1→S2→S4，该路径上的状态转换(如S1→S2)过程为一个Request，在测试过程中，数据生成模块将对Request的格式或内容进行模糊化，生成多个Request，由于一个变异的 Request只对应一个Session，因此在测试过程中，S1→S2的转换即会有多个会话过程(如图 6)。

[0039] 3.监控器模块

[0040] 监控器模块和驱动模块组成了框架的辅助部分。驱动模块主要与待测目标服务器通信，发送测试请求并接收服务器响应消息。监控器模块分为进程监控器、网络监控器、虚拟机控制器三个监控工具(如图7)。这些监控器必须与待测程序运行在同一台计算机上，称为被测机。而数据生成和会话管理与驱动部分可以运行在另一台计算机上，称为测试机。

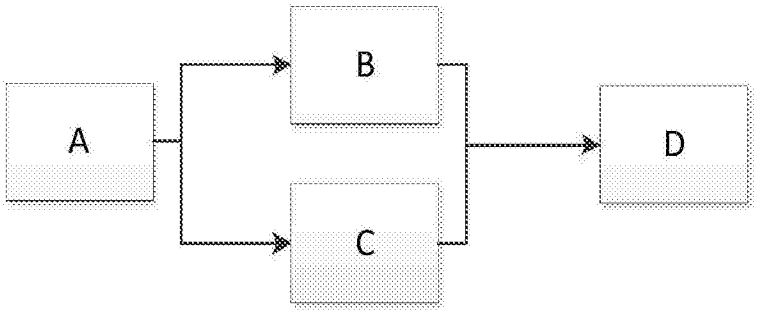

A
B
C
D

图1

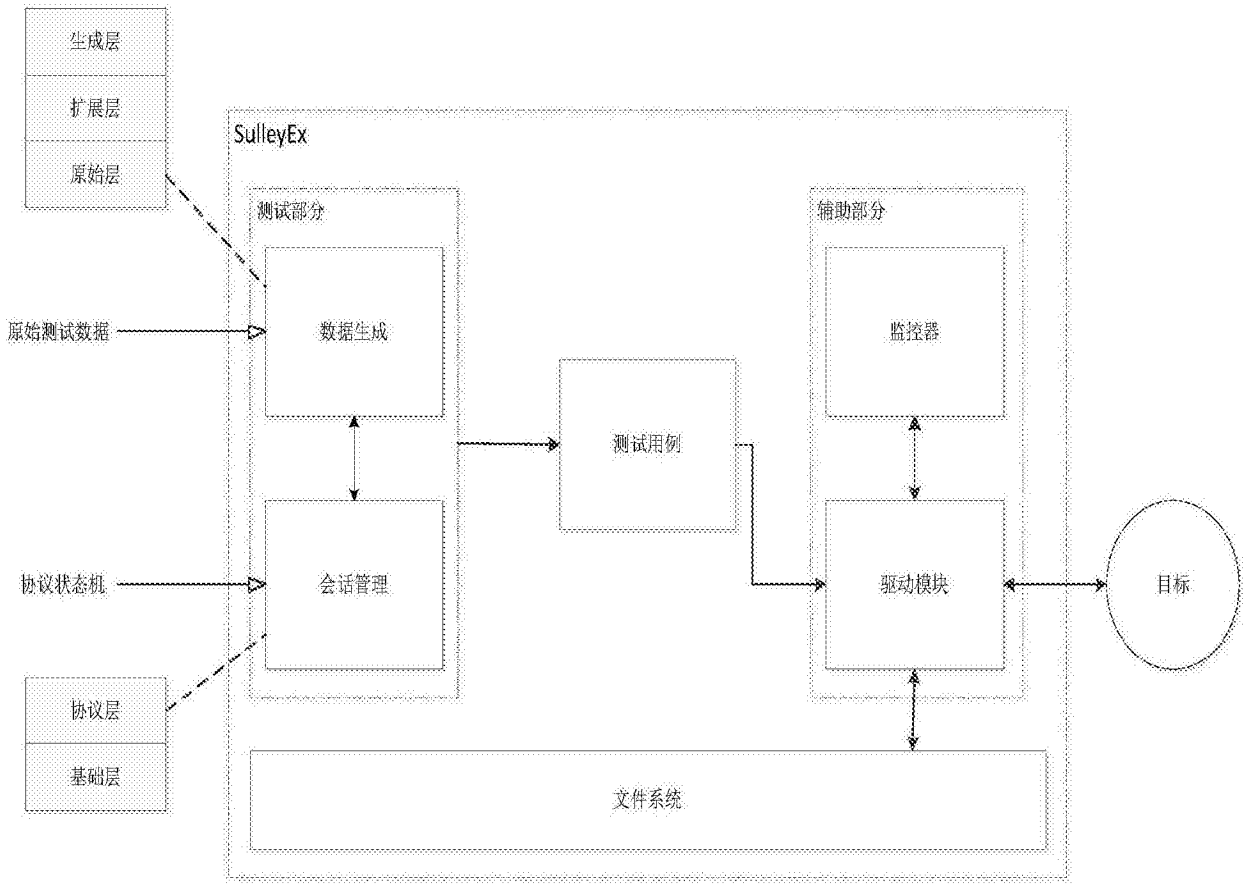

生成层
扩展层
原始层
SulleyEx
测试部分
辅助部分
原始测试数据
数据生成
监控器
测试用例
协议状态机
会话管理
驱动模块
目标
协议层
基础层
文件系统

图2

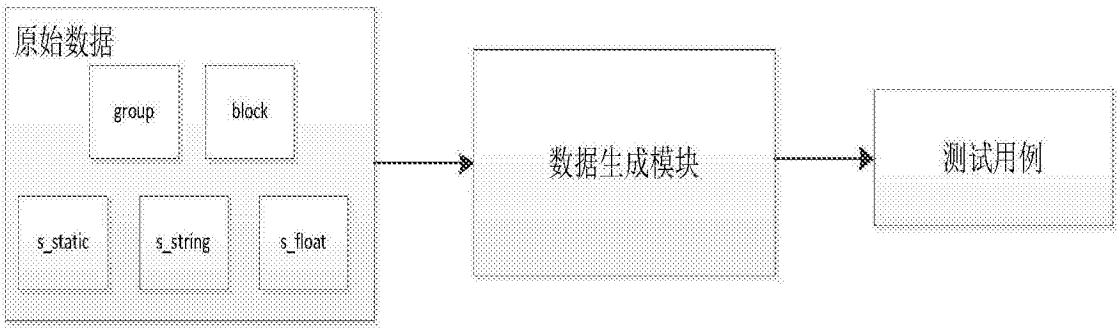

原始数据
group
block
s_static
s_string
s_float
数据生成模块
测试用例

图3

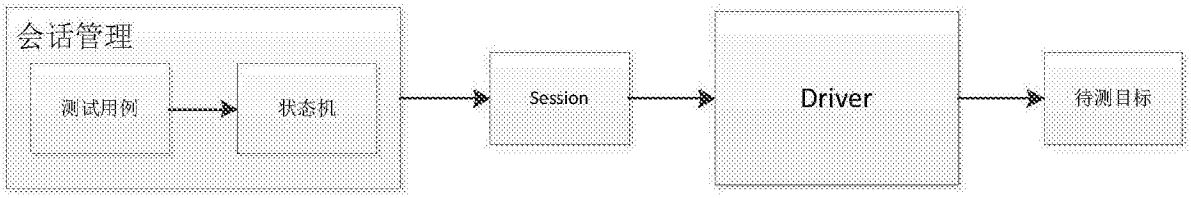

会话管理
测试用例
状态机
Session
Driver
待测目标

图4

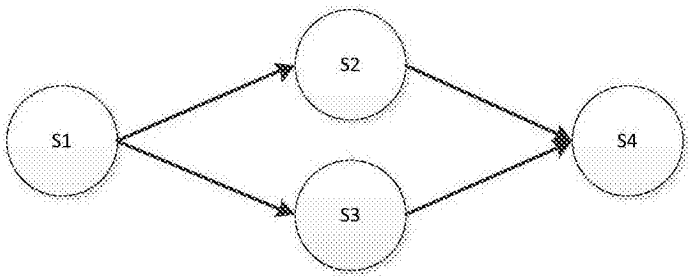

S1
S2
S3
S4

图5

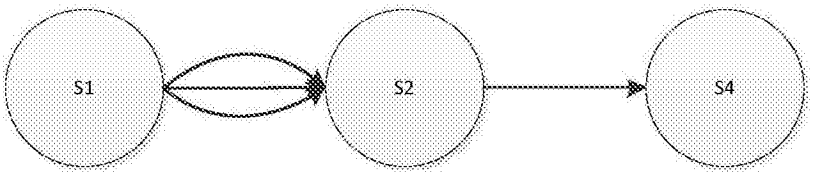

S1
S2
S4

图6

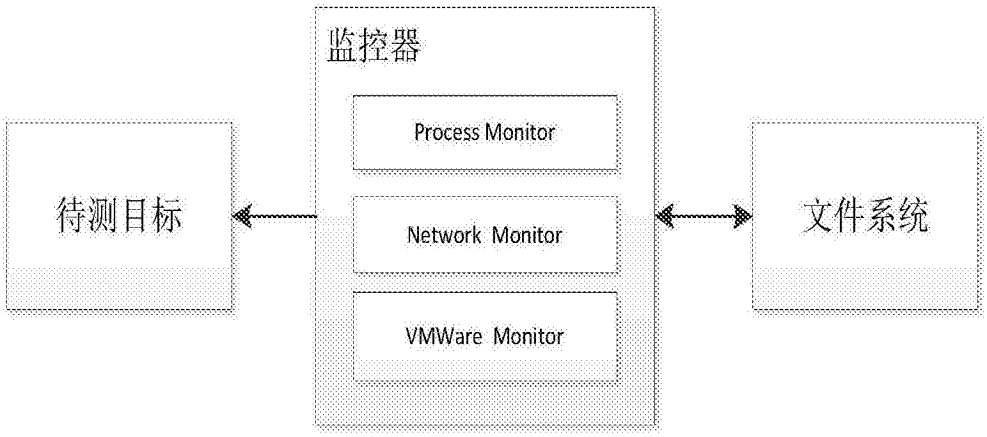

监控器
Process Monitor
Network Monitor
VMWare Monitor
待测目标
文件系统

图7