基于模糊测试的软件漏洞检测方法

颜汉权

摘　要：模糊器测试框架是一种通用的数据库，可以对各种不同的试验对象进行归纳。本文对模糊测试的流程进行了介绍，重点分析了在软件漏洞检测中的模糊测试方法，提出了软件漏洞检测中的模糊测试内容，以便更好的用于软件漏洞检测中。

关键词：模糊测试；软件漏洞；检测

1. 模糊测试流程

（1）确定测试的对象和输入的矢量。模糊测试是针对确定的程序进行的检测技术，因此，在进行模糊测试之前要先确定好需要测试的程序。一般来说，漏洞的产生绝大多数是由用户直接或间接造成的，有可能是因为接收的一些信息，也有可能是错误运行了程序。所以，一定要确定好输入的微量，这是影响到测试结果的关键步骤。

（2）生成模糊测试数据。在确定了程序和输入矢量之后，就可以生成测试数据，然后由系统根据数据自动选择测试数据方式。

（3）执行模糊测试数据。这一步会与上一步生成测试数据并行进行，执行过程一般包括启动目标程序、发送测试数据到目标程序等。同样，在这个过程中实现自动化也是必需的和十分重要的。

（4）监测异常。在进行模糊测试的时候，一定要注意监测异常。如果不能对检测过程中的异常进行监测并加以分析，可能会导致服务器崩溃，那么就影响了检测的准确性。监测还能对源数据进行分析，从而发现其中存在的未被发现的异常。

（5）确定可利用性。一旦检测到异常，首先应该查找异常出现的地方，然后分析其原因，解决异常。这些步骤就需要手工来完成，而且也需要具备丰富的知识。

2. 模糊测试方法

模糊器主要分为基于变异的模糊器和基于生成的模糊器两种，基于变异的模糊器主要是对已有的数据进行改变来创建测试用例，基于生成的模糊器是指通过协议或者文件格式来进行变异，从而创建测试用例。同时，我们还可以把模糊测试方法分成以下4类。

（1）预生成测试用例。这种方法要求在使用前对测试对象的相关数据进行分析，因此，这用这种方法进行测试之前需要进行大量的工作，这可能在一定程度上延长了检测时间。这种方法没有引用随机制，因此不能生成很多的测试例子。

（2）随机方法。这种方法是效率最低的，正是由于它的随机性，使得它不能全面地对软件进行测试。不过这种方法可以快速地发现漏洞，但是具有较大的运气成分。对一个比较大的数据包，不推荐采用这种方法，因为这种方法有一定的不可靠性，用这种方法对较大的数据包进行检测，就会使检测时间变得很长，不利用接下来的工作，影响了检测效率。

（3）人工协议变异测试。这种方法一般是用于测试Web应用软件的。这种方法依靠经验的成分比较高，因此，它需要对经验进行总结并记录存档。其实这就是通过人工输入数据来找出漏洞的，因此，它比随机方法还要简单，但是自动化不强。

（4）自动化变异或暴力测试。这种方法具有一定的强制性，因为它能够强制代码覆盖在测试结果为良好的程序上，然后再进行检测。但是，这种方法的检测效率是比较低的，因为在检测过程中，系统会处理很多根本无效的数据，这样就会延长测试时间，拖慢进度。不过，这种方法在这些问题上还是有一定的缓解能力的，因为这种方法是可以全程利用自动化的原理的。

3. 模糊器类型

（1）本地模糊器。命令行参数和环境变量是将变量引入到程序中的两种最基本的方式，因而针对setuid应用程序的模糊器可分为两类：命令行参数模糊器和环境变量模糊器。还有一类本地模糊器是文件格式模糊器。很多应用程序在处理畸形文件时可能会出现异常，这就需要文件格式模糊器来参与监测。其中，浏览器模糊器是一种特殊的文件格式模糊器，它通常利用HTML的功能来实现模糊测试过程的自动化。

（2）远程模糊器。远程模糊器的测试对象为基于网络的应用程序，诸如各类服务器软件。这类应用程序一直以来都是模糊测试最重要的测试对象。远程模糊器主要包括网络协议模糊器和Web应用程序模糊器。网络协议模糊器被分为两类：以简单协议为测试对象的模糊器和以复杂协议为测试对象的模糊器。Web应用程序模糊器已经成为访问后端服务的一种流行方式，这些后端服务包括电子邮件等网络服务。

（3）模糊器框架。模糊器测试框架实际上就是通用的数据库，可对于各种不同的试验对象进行归纳统计，因此，可运用的范围和领域较广，能够针对不同的类型目标进行分析。

参考文献：

[1]夏一民，罗　军，张民选．基于静态分析的安全漏洞检测技术研究[J]．计算机科学，2006（10）．

[2]李永华，窦春铁．谈计算机安全漏洞动态检测的原理方法与实践[J]．数字技术与应用，2010（07）．

（作者单位：惠州市广播电视大学）