基于模糊测试的软件安全漏洞发掘技术研究

刘　彪

（69230部队　新疆　833000）

【摘　要】近年来，随着计算机网络技术的不断推广和应用的普及人们生活和工作越来越离不开计算机技术。目前，各行各业的发展都逐渐实现信息化。在当今互联网络时代，计算计研究工作仍然在不断深入，很多新专业软件层出不穷，但是软件的安全性是人们高度重视和思考的问题。因此，本文主要分析了模糊测试的定义，阐述了软件安全漏洞存在的危害性。针对模糊测试的软件安全性进行深入的研究，最后，通过软件安全测试试验分析静态测试和动态测试状态下，并且通过本文的研究，对未来模糊软件安全漏洞发掘技术的相关研究进行展望。希望通过本文的分析能为模糊软件安全漏洞发掘技术的研究和推广奠定坚实的基础。

【关键词】模糊测试；软件安全；安全漏洞；发掘技术

中图分类号：TP311.53　　**文献标识码：A**　　**文献编号：1009-6833（2014）03-037-02**

Excavation technique based on fuzzy test software security vulnerabilities

Liu Biao

Abstract: In recent years, along with the further promotion of computer network technology and application of the spread of people's life and work more and more inseparable from the computer technology.At present, the development of all walks of life are gradually realize the informationization.Computer research work in the Internet era, still further, a lot of new professional software emerge in endlessly, but the software security is people attaches great importance to and thinking of problem.Therefore, this article mainly analyzes the definition of fuzzy test, this paper expounds the harmfulness of software security vulnerabilities exist.In view of the fuzzy test software security in-depth research, finally, through the analysis of static testing and dynamic testing of software security testing experiment condition, and through the research of this paper, fuzzy software security hole excavation technology for the future research were discussed.Hope that through this article analysis for research and popularization of the technology of fuzzy software security vulnerabilities discovered lay a solid foundation.

Keywords: fuzzy test; Software security; Security vulnerabilities; Excavation technology

0　引言

随着人类社会信息时代的带来，计算机技术已经延伸到人们生活的各个方面、各个领域，软件安全漏洞却无处不在，在计算机安全防卫技术水平不断提高的同时，很多电脑黑客以及病毒软件也得到相应的发展。因此，软件安全管理工作非常重要，直接关系着用户信息安全和企业信息安全。

1　模糊测试的软件安全漏洞

1.1　使用者权限漏洞

模糊测试软件安全漏洞使用者权限漏洞是由于使用者以不正当的手段或者在比较复杂的运行环境下，继续运行自己的网络，导致安全受到外界的干扰和影响。正是由于使用者这种违法使用的行为，给软件安全带来很大的隐患。一旦使用这权限发生漏洞，当在不安全的网络环境下运行，系统内部的资料就会受到威胁，有时候将会破坏甚至使整个系统无法正常运行。

1.2　核心系统监控漏洞

核心系统监控漏洞是系统核心的工作环境出现无法配合软件系统需求的现象，由于不能读取系统资源，导致很多重要的数据信息泄露，由于系统不能正常运行。核心系统监控的安全漏洞将直接威胁整个网络安全和运行，计算机系统中所有软件储存的地方均在核心系统中。因此，核心系统的监控是最为关键的部分和环节。

2　模糊测试的软件安全漏洞发掘技术的应用构想

由上述可知，模糊测试的软件安全漏洞存在的最根本原因是由于程序单元上的问题，因此，研究安全发掘技术，要朝向这个方向深入挖掘。

2.1　主要程序结构

根据目前已有的计算机技术，针对问题存在的根源，相关技术人员结合实践经验，初步建立安全软件测试框架。安全漏洞发掘技术主要是由于单元测试、集成测试、系统测试和敏测试等几个部分共同构成，经过计算机软件的数据需要经过层层的测试，减少安全漏洞问题这种结构框架属于一种局部性安全漏洞程序管理方式，是安全漏洞检测的前期阶段，该阶段所检测出来的漏洞、漏洞区域或者范围，都是后期连续测试的工作参考依据。因此，为了控制安全漏洞问题的延伸，应该认真做好检测工作，避免缺失增加后期维护工作。

2.2　安全漏洞发掘模型

安全发掘技术将程序测试分为单元测试、集成测试、系统测试以及域测试，其安全测试贯穿整个测试过程，模糊测试方式由上述几种模糊器选择最佳的一种方式。首先，建立数据样本应用变异技术测试模型，在自动生成的模糊器上，数据出入之后，将会在制定域内形成规范的文件格式，在建立的测试模型中，采用随机方法，协议变异人工测试，然后通过测协议，得出生生成测试的结果。预生成的测试用例是基础和前提，在此基础之上能对系统中的数据文件或数据包进行测试，测试边界环境是否安全，是否存在安全威胁或违法事件。全程的数据测试能提高测试的精确度，提高整个系统的安全系数。其次，通过模型的初步测试之后，再采用协议变异人工测试需要进行干预测试，测试人员应该对系统或软件有足够的了解，向数据包或者文件发送测试指令，对目标进行测试。最后就是高级测试，即对两种不同形态进行测试。先开展静态测试，其重点测试测范围是逻辑运行中的网络安全。静态测试直接采用程序分析法，对程序中的源代码直接进行测试和分析，比较在不同网络环境下，区域性程序安全漏洞检测，需要通过程序语言和程序分析器，对系统协议或者数据包的安全漏洞进行检测。而动态测试就是在静态测试的基础之上，透过静态测试找到的安全漏洞问题，利用自动化协助安全漏洞检测工作，对具体检测功能和运行上存在的漏洞开展安全检查，测试规划使用异常格式、容量或负载等作为传输硬件资源的纽带，在测试人员操作下，根据测试目标实测情况科学舍取，最终，形成动态测试。整个

（下转第40页）

然后，每个属性$u_j(j=1,2,\ldots,m)$为一随机变量，综合考虑物联网的整体属性，使用均方差法客观对各属性权重进行赋值，构造权值向量$w^1=(w_1^1,w_2^1,\ldots,w_j^1,\ldots,w_m^1)^T$，$w_j^1\in[0,1]$，$\sum_{j=1}^{m}w_j^1=1$。具体步骤如下：

（1）求随机变量u_j的均值：$E(u_j)=\frac{1}{n}\sum_{i=1}^{n}r_{ij}$。

（2）求u_j的均方差：$D(u_j)=\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(r_{ij}-E(u_j))^2}$。

（3）求u_j的权数：$w_j^1=\frac{D(u_j)}{\sum_{j=1}^{m}D(u_j)}$。

最后，为了在用户个性化需求和物联网的整体属性间找到一合适平衡点，构造权值向量$w=(w_1,w_2,\ldots,w_j,\ldots,w_m)^T$，$w_j\in[0,1]$，$\sum_{j=1}^{m}w_j=1$。其中$w_j=\frac{1}{2}w_j^1+\frac{1}{2}w_j^2$为最终使用的权值向量。

2.3 对方案进行排序和决策

物联网具有属性多、方案多的特点，在进行排忧计算时必须考虑计算量的问题，并且要求最优方案必须优势明显，即最优解和次优解的距离必须要足够大。根据以上特点，本文选择几何加权平均(OWGA)算子。

利用OWGA算子对各方案的属性值进行集结，求得其综合属性值v_i，

$$v_i=OWGA(r_{i1},r_{i2},\ldots,r_{in})=\prod_{j=1}^{n}(r_{ij})^{w_j}$$

其中b_j是一组数据$r_i(i\in N)$中第j个最大元素，

然后按照$v_i(i\in N)$的大小对方案进行排序并进行决策。

3 总结与展望

本文结合物联网环境下系统响应的特点，引入决策科学中的多属性决策思想，实现了终端的自动响应，并且通过巧妙地提出了合适的信息结算引子，直接使用输入的实数数据进行决策，节省了信息的量化判断成本，具有良好的可操作性。

参考文献：

[1] Green TJ，Tannen V.Models for incomplete and probabilistic information[J].IEEE Date Engineering Bulletin，2006，29(1)：17-24.

[2] Blumensath T，Davies ME.Iterative hard thresholding for compressed sensing[J].Applied and Computational Harmonic Analysis，2009，27(3)：265-274.

[3] 王永庆.人工智能原理与方法[M].西安：西安交通大学出版社，2006.

[4] 黄海生，王汝传.基于隶属云理论的主观信任评估模型研究[J].通信学报，2008，29(4)：13-19.

（上接第37页）

模糊软件安全漏洞测试发掘模型如图1所示。

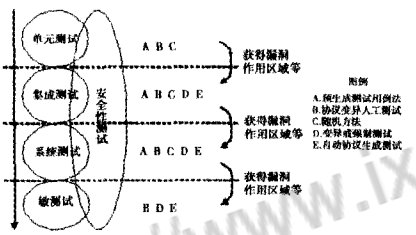

图1 安全漏洞测试发掘模型

3 结束语

综上所述，在信息时代快速发展的形势下，软件安全已经成为人们高度重视和关注的问题，软件安全直接关系着各行业内部的机密文件的安全，内部网络一旦被入侵，将会破坏整个系统。因此，研究模糊软件的安全漏洞发掘技术具有重要的作用和意义，笔者结合自身的工作经验和相关研究结果，对安全发掘技术进行深入的研究，提出要确保模糊软件的安全，应该要重点研究和发掘系统的逻辑控制程序。根据目前已有的计算机技术，笔者指出，随着计算机技术人员研究的不断深入，最终必定能实现模糊软件安全发掘技术的推广和应用。

参考文献：

[1] 倪凯斌.基于Fuzzing的IE浏览器控件安全漏洞发掘技术研究[D].暨南大学，2010.

[2] 黄奕.基于模糊测试的软件安全漏洞发掘技术研究[D].中国科学技术大学，2010.

[3] 苏恩标.基于数据块关联模型的漏洞发掘技术研究及应用[D].电子科技大学，2010.

[4] 张晛譞.基于Windows平台的软件安全漏洞发掘技术研究[D].电子科技大学，2010.

[5] 刘金刚.模糊测试下软件安全漏洞发掘技术分析[J].网友世界，2013(04).

[6] 刘为.基于模糊测试的XSS漏洞检测系统研究与实现[D].湖南大学，2010.

[7] 苑立娟，张育玉.基于模糊测试的软件安全性测试框架的研究与设计[J].煤炭技术，2010(08).

作者简介：

刘彪（1984—），男，湖南永州人，大学本科，研究方向：计算机网络安全技术与现代通信技术应用。

（上接第38页）

为互联网、文件、电子邮箱等多种传播形式，扩大了计算机病毒的传播范围。随着计算机病毒种类的不断增加，我们除了开发与安装更加有效的杀毒软件之外，还可以进行相应的系统更新，确保计算机网络的全面安全，保证用户信息的安全性。一旦出现一些新病毒，就要及时采取一些解决措施，保证可以在最短的时间内解决问题，恢复系统运行，找回丢失数据等。

3.4 运用文件保密技术

在进行文件加密的时候，可以由明文转换成密文，是保证计算机网络安全的有效措施之一，确保了数据传输的安全性。现阶段，计算机网络中应用的加密技术主要包括三种：链路加密技术、端点加密技术、节点加密技术。在计算机运行过程中，数据加密技术得到了普遍的应用，不仅可以保证网络信息传输的安全性，还可以提高网络信息的真实性。

4 结束语

总而言之，随着信息技术的快速发展，网络化的迅速发展，网络给人们的生活带来了很大的变化，同时也带来了一定的威胁。人们在利用网络进行工作与学习的时候，也越来越重视网络安全问题。在研究计算机网络安全的时候，一定要对影响其安全性的因素分析，这样才可以进行针对的改进，提出相应的防范措施，保证网络安全。同时信息加密技术也是一项非常重要的防范措施，有效保证了计算机网络运行的安全性与可靠性。

参考文献：

[1] 李晓利.数据加密技术在计算机网络安全中的应用探讨[J].数字技术与应用，2011(06).

[2] 刘乔佳.小议信息加密技术在计算机网络安全中的应用[J].计算机光盘软件与应用，2012(16).

[3] 朱闻亚.数据加密技术在计算机网络安全中的应用价值研究[J].制造业自动化，2012(03).

[4] 潘芳.基于信息安全的现代信息加密技术研究[J].信息安全与技术，2011(10).

[5] 田瑞霞，王烽.数据加密技术在计算机网络中的应用探讨[J].信息安全与技术，2014(02).

[6] 王佳煜.有关信息加密技术在计算机网络安全中的应用研究[J].计算机光盘软件与应用，2012(09).

作者简介：

李书香（1975—），女，毕业于计算机专科学校，常宁市职业中等学校任职，研究方向：计算机技术及应用。