论高可靠性系统中软件容错技术的应用

# **摘要：**

2016年3月，我公司承担了国家某安全中心漏洞挖掘系统的开发工作，我在该项目中承担系统架构设计师的职务，主要负责系统的架构设计。该项目的主要目的是依托大数据平台从互联网流量中挖掘未知漏洞。

本文以漏洞挖掘系统为例，从多个角度对系统的可靠性进行了分析，重点讨论了两种软件容错技术。针对互联网流量的需要实时捕获，在流量捕获模块中采用了双机热备技术；针对漏洞数据需要永久存储不丢失，在数据存储方面采用了RAID5机制；针对漏洞识别的准确性，在漏洞判定部分采用了N版本程序设计方法；此次之外还对采取恢复块方法、防御式程序设计及集群部署等方法。通过以上多种措施，保证了系统的可靠性。目前系统已稳定运行一年多，从而验证了该项目采用可靠性技术的正确性。

# **正文：**

随着互联网的快速发展，网络上出现的安全问题越来越多，从互联网发展至今，已经爆发了众多的网络攻击事件，如网络蠕虫病毒感染、主机被控制、数据库被非法访问、非法电子银行转账等等。针对这些安全问题，很有必要开发一种web漏洞的发现和利用技术。2016年3月我公司承接了国家某安全中心漏洞挖掘系统的开发工作。该项目通过对互联网中的流量进行特征分析，从中提取出相关的攻击内容，并将这些内容存储到大数据平台，结合大数据分析技术，对攻击者进行跟踪分析，从而捕获出未知漏洞。通过这种漏洞挖掘技术可以极大的解决大数据，大流量背景下web攻击入侵，帮助用户做好“事中”的安全工作，协助安全厂商对互联网攻击进行针对性过滤。

系统在整体架构上采用了面向服务的架构SOA。前端采用了PHP进行开发，后台流量分析工作采用运行性较教高的c语言在Linux服务器上开发，流量包存储使用了企业磁盘阵列，数据存储采用了mysql。通过将系统拆分为多个子模块，各个子模块的构建上用服务进行了封装，它们之间通过消息进行通信。经过对客户需求的分析，我将该系统拆分为了流量捕获模块（负责从互联网中捕获流量）、pcap文件存储模块（负责将互联网中的流量存储到大数据平台）、流量分析模块（负责对流量进行分析验证）、数据库模块（负责漏洞数据的存储）和web管理模块（负责下发漏洞规则和查看漏洞信息）。

按照合同规定该项目开发工作必须在一年内完成，在保证系统功能及性能的基础上，对系统的可靠性提出了要求。在可靠性方面要求：1. 实时捕获流量要求系统出现故障宕机不能超过5分钟；2. 系统提取出的漏洞及对应的流量不能丢失；3. 系统对漏洞识别准确率需要达到90%以上。

系统的可靠性是系统在规定时间内及规定的环境条件下，完成规定功能的能力，也就是系统无故障运行的概率。为了保证系统的可靠性，必须采取相应的容错机制。容错技术分为结构冗余、信息冗余、时间冗余等。其中结构冗余包括硬件冗余和软件冗余。信息冗余是通过校验码来实现，时间冗余通过重复多次进行相同的计算来实现。提高系统可靠性的技术主要有N版本程序设计、恢复块方法、防卫式程序设计、双机热备、集群技术及冗余设计。项目中我根据客户对系统可靠性的要求从以下几个方面进行了分析。

针对系统需要实时捕获流量，流量捕获系统7\*24小时正常运行。我们在流量捕获模块采用了双机热备。在系统中部署两台流量捕获系统，一台作为主流量捕获系统，一台作为备用系统，两个系统之间通过心跳线连接。当流量捕获主系统出现故障的时候，立即将流量捕获工作切换到备用系统中，实现了系统的无缝切换，从而保证系统的可靠性。针对捕获的有价值漏洞原始数据和漏洞数据不丢失，我对数据存储采取了企业磁盘阵列，采用了raid5 N+1网络存储技术，即便磁盘坏了一个，也可以进行恢复。由于每天需要处理的网络流量大约30TB，在这里我们才用了5台10TB硬盘挂载到服务器上。除硬件上采取的措施外，软件上我们也做了特别的容错技术来提高系统的可靠性。下面从软件容错的两种方法详细讨论它在可靠性的中应用。

N版本程序设计

N版本程序设计的思想是相同的需求，使用不同的人来做设计和编码。开发出几个不同的版本，各自验证正确后，通过表决器比较各个版本执行的结果。采用少数服从多少的策略，这样可以将某个偶然出现的错误屏蔽掉，这种方法实时性非常高，实现代价也比较大。一般只会用在程序模块的重要性特别高，一旦计算错误将会出现严重后果的模块。在本项目中，考虑到本项目开发人员的紧缺性，使用该方法虽然可以提高漏洞识别率，但是将增加项目成本。而客户又对漏洞判定的准确性提出了很高的要求。基于以上考虑，我将系统中特别重要的漏洞判别模块采用了该方法，在本项目针对sql注入漏洞的判别，不同的安全开发工程师都有各自不同的理解及各自的判定方法，通过将判定工作分给三名安全开发工程师进行背对背开发，开发出三个不同版本的漏洞判定程序，每个程序对漏洞判定都设定了高危（积分为5分）、风险（积分为3分）和未知（积分为1分）和安全（积分为0分）4个不同级别。当3个版本的总积分大于等于8分则认定为高危漏洞；当总积分小于4分认定为安全。通过该方法大大提高了漏洞的识别率。

恢复块方法

恢复块方法的思想是首先设计好几个备用块，选取其中一个作为主块。首先执行主块，当主块执行不合格后，再执行后备块1，后备块1执行不合格，再执行后备块2，依次类推，直到输出正确结果为止。它是一种后向恢复的策略（将系统恢复到一个正确的状态，继续执行），其特点是由于主块可能执行不合格，可能要执行多个恢复块，故实时性比较差。这种方法对验证模块的正确性要求也非常高，实现代价也比较大。在该项目中，由于系统对流量的处理要求在12小时内处理完成，对系统的实时性要求不是很高。在该项目中进行流量抓包的时候，可能捕获到异常的包，有的甚至不是一个完整的http请求，程序在处理这类异常包的时候，只对能获取五元组的数据包进行分析。在使用恢复块方法中，主块用于处理完整的http请求，并根据请求的动作和漏洞规则匹配输出正确结果；后备块1用于处理只有http请求的包，根据请求规则例如sql注入、xss跨站攻击等行为进行匹配输出，输出正确结果，后备块2用于处理只有http响应的包，根据响应的规则例如数据库账号，进行匹配输出，后备块3用于处理其他异常的包，并进行五元组统计。通过该中方法，大大提高了系统的可靠性。

除了以上几个方面的考虑外，对整个系统采用了防卫式程序设计、防御式编程技术，同时也考虑了集群技术。在指定预算的情况下，针对系统的性能，对使用高性能主机和使用分布式集群进行了思考。但是考虑到系统的可扩展性及可靠性，我使用了分布式集群技术。通过使用消息队列，对流量分析模块进行了分布式部署，各个模块通过从消息队列中取出消息进行处理。通过使用该分布式集群部署流量分析模块，当其中一台服务器出现故障的时候，其他服务器还可以从消息队列中取出消息进行处理，避免了因为服务器单点故障导致系统性能及可靠性下降。除了采取以上的措施外，我们还通过加强测试，增加检查机制来保证系统的可靠性。

该项目开发工作于2016年8月完工，系统上线后，我们的安全分析人员和客户使用该系统对互联网流量进行漏洞挖掘，一共产生了150种以上的web流量攻击流量特征和5个未知web漏洞。在国家某安全中心网研室的其他项目中起到了支撑作用，尤其是某变量覆盖漏洞、某文件写入漏洞，某sql注入漏洞在项目使用过程中取得了一定得效果，得到了好评。为开展互联网安全事件得防御、发现、预警和协调处置等工作提供了数据依据，更好的维护了国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

在项目开发完成进行漏洞挖掘期间，系统的运行非常好，除了常规系统维护，很少出现系统故障，满足了客户对系统的可靠性要求。该项目在保证系统可靠性方面使用了双机热备、RAID5磁盘阵列、N版本程序设计、恢复块方法、防御式程序设计及集群技术。经过验证，这些措施都十分正确的。

转自：https://blog.csdn.net/feitianxuxue/article/details/78918749