论软件系统架构评估

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，论述了软件系统的架构评估。首先分析了软件架构评估所普遍关注的质量属性并阐述了其性能、可用性、可修改性和安全性的具体含义。整个系统采用了面向服务 SOA 的架构设计方法。在架构设计完成之后，对 SA 评估采用了基于场景的评估方式中的体系结构权衡分析方法 ATAM，并详细描述了其评估过程，项目评估小组经过对项目的风险点、敏感点和权衡点的讨论后生成了质量效应树。目前系统已稳定运行一年多，从而验证了该项目采用 ATAM 架构评估保证了系统的顺利完成。

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）。下面先介绍下软件架构评估的质量属性。

架构评估是软件开发过程中的重要环节，在软件架构评估中的质量属性有：性能、可用性、可修改性、安全性、可测试性、可靠性和易用性等。其中前 4 个质量属性是质量效应树的重要组成部分。性能是指系统的响应能力，即经过多长时间对事件做出响应。可用性是指系统能够正常运行的比例，通过用两次故障之间的时间长度或出现故障时系统能够恢复的速度来表示。可修改性是指系统能以较高的性价比对系统做出变更的能力。安全性是指系统能够向合法用户提供服务，同时拒绝非授权用户使用或拒绝服务的能力。

常用的架构评估方法有：基于问卷调查的评估方式、基于场景的评估方式和基于度量的评估方式。基于问卷调查的评估方式是由多个评估专家通过调查问卷的方式回答问卷中的问题，对多个评估结果进行综合，最终得到最终结果。其评价的具有主观性不太适合本项目。基于度量的评估方式虽然评价比较客观，但是需要评估者对系统的架构有精确的了解，也不太适合本项目。而基于场景的评估要求评估者对系统中等了解，评价比较主观，故本项目采用了基于场景的评估方式。基于场景的评估方式又分为架构权衡分析法 ATAM，软件架构分析法 SAAM 和成本效益分析法 CBAM。本项目中根据不同质量属性使用了 ATAM 作为系统架构评估的方法。

在使用 ATAM 进行架构评估时，我们根据项目需要成立了项目评估小组。其主要成员包括：评估小组负责人、项目决策者、架构设计师、用户、开发人员、测试人员、系统部署人

员等项目干系人。我在这里的身份是项目的评估小组负责人和首席架构师。架构的评估经历了描述和介绍阶段、调查和分析阶段、测试阶段和报告阶段四个阶段。下面我分别从这四个阶段进行介绍。

在描述和介绍阶段，由于项目评估成员有部分人员对 ATAM 并不熟悉，我首先介绍 ATAM 的方法。它是一种基于场景的软件架构评估方法，对系统的多个质量属性基于场景进行评估。通过该评估确认系统存在的风险，并检查各自的非功能性需求是否满足需求。客户也阐述了系统的目的和商业动机。项目是为了通过捕获互联网流量从而挖掘出有价值的漏洞信息。通过实时获取漏洞可以有效的展开防御，保证网站的安全性。客户关注系统的性能及系统能否获取高质量的漏洞信息。最后作为架构设计师的我描述了系统将要采用的 soa 架构，并将系统进行了拆分，并讲解了各个子模块的功能，初步决定系统服务端在 Linux 下使用 c 语言进行开发。

在调查分析阶段，不同的需求方基于各自的考虑都提出了各自的要求。其中客户方提出：系统的要保证其可靠性，特别是针对黑客 ip 进行跟踪的时，系统发生故障必须在 1 分钟内恢复，此优先级最高。经过自动化分析，系统对漏洞的自动识别率必须达到 90%以上，此优先级较高。系统可以对规则模块实时进行修改，其修改工作必须在 1 人天完成，以便可以根据最新的规则进行漏洞捕获。系统要确保一定的安全性。安全分析人员提出：系统需要过滤大部分正常的流量，以减轻安全分析人员的分析难度。系统必须提取出有价值的高风险 ip，无效的流量跟踪将会带来产出的低下。开发人员提出为了保证系统的开发效率及系统修改性，可以进行并行开发。经过总结我们获得了系统的质量效应树如下（考试时回简要图）。

针对这些场景我们分析了项目开发过程中的风险点、敏感点和权衡点。经过分析，该项目中存在以下风险点：黑客的 ip 如果不能实时捕获，将会丢失重要漏洞信息；系统中对消息的处理如果超过 12 小时，将会产生大量的消息积压。敏感点有：用户的加密级别、漏洞规则的修改。权衡点有：改变漏洞规则的严格程度会提升漏洞的准确率，同时带来系统性能的下降。改变系统的加密级别对系统的安全性和性能都会产生影响。

在测试阶段：经过评估小组集体讨论，确定了不同场景的优先级如下：系统的可用性最高，性能其次，可修改性及安全性优先级较低。在保证系统可用性方面，在流量捕获部分使用双机热备技术，在两个捕获系统之间设置心跳，当一台捕获系统出问题，另一台捕获设备接管。在流量自动化分析部分，采用了集群部署技术，一台分析设备出问题，不会影响整个分析系统。在保证数据安全性方面，磁盘采用企业磁盘阵列 raid5 机制。在用户数据安全性方面，采用了非对称加密及信息摘要技术。

最后形成了评估报告，经过对架构的评估，确定了系统的风险点、敏感点、权衡点和非风险点，最后以文档的形式表现。其包括的内容包括：架构分析方法文档、架构的不同场景及各自的优先级、质量效应树、风险点决策、非风险点决策及每次的评估会议记录。

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。