软件所在内嵌脚本解释器的漏洞自动化挖掘研究中取得进展

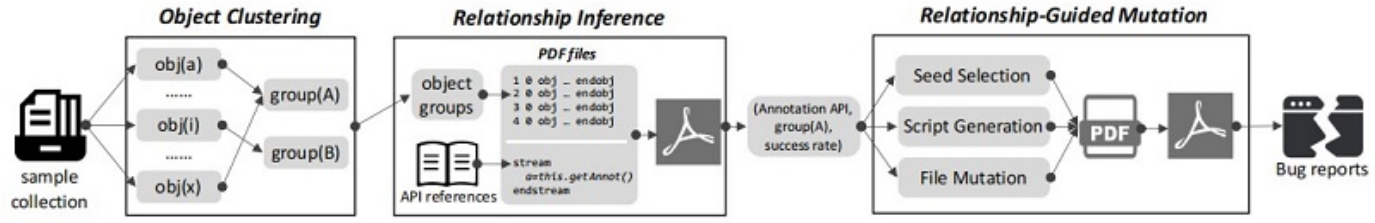
文章来源：可信计算与信息保障实验室 | 发布时间：2022-01-24 | 【打印】 【关闭】

近日，中国科学院软件研究所可信计算与信息保障实验室在内嵌脚本解释器的漏洞自动化挖掘研究方面取得进展。该研究提出了基于关联变异的漏洞挖掘方法，能够有效地挖掘软件与脚本引擎之间绑定代码的漏洞，在大型商用文档软件的安全性测试中发挥重要作用。

近年来，像JavaScript这样的脚本语言正在被集成到商业软件中，以提供统一的接口。例如，Adobe Acrobat接受JavaScript来动态操作PDF文件。为了弥合高级脚本和实现软件的低级语言(如C/C++)之间的距离，需要一个绑定层来进行数据的传输和转化。但是，由于双方的复杂性，绑定代码容易出现语义不一致和实现错误，从而导致严重的漏洞。现有的测试绑定代码的工作仅仅集中在脚本端，因此不能有效挖掘需要特殊内容对象输入才能触发的漏洞。

针对该问题，团队提出了基于内容对象和脚本之间关系的关联性变异方法，通过同时修改内容对象和脚本代码，来触发脚本解释器中绑定代码中的漏洞。团队认为许多软件中的漏洞都是由于程序初始状态和动态操作之间的相互作用的不一致性造成的，而这种不一致性只能通过关联性突变来触发。团队提出了3个方法来实现脚本语言与内容对象的关联性变异:首先对内容对象进行语义相似性聚类，来减少内容对象的搜索空间；其次，基于大量原始样本测试执行，通过统计学习的方法推测出脚本代码与对象类之间的关联关系；最后，利用推断出的关系选择合适的内容对象和相关联的脚本代码进行关联性变异。基于该工作的原型系统COOPER应用于三个应用广泛地集成了内嵌脚本语言的商业软件中，包括Adobe Acrobat, Foxit Reader和Microsoft Word。COOPER系统成功发现了134个未知漏洞。该团队已经将全部漏洞报告给了相关软件产商。其中，56个漏洞已经被修复，33个漏洞已被分配了CVE编号，团队多次被漏洞相关厂商公开致谢。

相关成果以“COOPER:Testing the Binding Code of Scripting Languages with Cooperative Mutation”为题被网络安全领域顶级学术会议NDSS2022接受。该论文的作者为软件所博士生徐鹏、奇安信技术研究院博士王衍豪、宾夕法尼亚州立大学助理教授胡宏、软件所研究员苏璞睿。该研究获国家重点研发计划等项目支持。



Cooper：内嵌脚本解释器的自动化漏洞挖掘框架