符号执行中高语句覆盖率的路径调度

http://www.firstlight.cn 2010-05-11

符号执行和约束求解相结合的软件测试方法采用深度优先搜索的路径调度算法会造成测试路径聚居性问题，实际软件中存在路径爆炸，使得采用该算法的测试语句覆盖率低下。提出一种新的PSHC路径调度算法。先将路径分为前缀和后缀两部分，每次测试总是试图寻找这样的路径，该路径与已存在的路径具有最短的相同前缀，并且包含尽可能多的尚未被访问过的基本块作为其后缀。基于Phoenix漏洞发掘工具的实验结果表明，PSHC算法可以迅速提高测试的语句覆盖率到100%，有效解决由于深度优先搜索的路径聚居性导致的测试代码的局部性问题，PSHC算法产生的路径数与循环深度无关，软件规模越大，该算法的表现越好。

存档文本

北京雷速科技有限公司 版权所有 2003-2008 Email: leisun@firstlight.cn