基于重放分析的网络协议软件状态变量自动化发现技术

黄见欣[1]，喻波[1]，刘润昊[1]，苏金树[1,2]
[1]国防科技大学计算机学院，中国长沙市，410073
[2]军事科学院，中国北京市，100091

摘要：网络协议软件通常具有程序路径复杂、状态空间庞大的特点。程序中往往存在着一些带有状态的关键变量，用于记录协议状态和会话信息。这些状态变量一旦处理不当，很可能违背协议规范，进而产生逻辑错误，导致协议软件出现潜在的缺陷或漏洞。本文针对现有程序分析技术难以发现网络协议软件中的状态变量，且自动化程度偏低的问题，提出一种基于重放分析的状态变量识别方法。考虑到状态变量主要反映着通信双方的参数和程序的状态，具有这些特征的变量通常会以全局变量或静态变量的形式，持续存在于进程之中，该方法通过记录和重放协议软件的执行轨迹，运用动态插桩技术，在协议状态和软件状态的变化过程中，分析内存关键区域的全局变量和静态变量的状态特征，并结合规则进行筛选判定。在此基础上，设计并实现了一套能够自动化发现状态变量的原型系统，在ProFuzzBench中的9个程序和2个现实中的复杂协议软件上进行了测试。实验结果显示，平均真正类率（TPR）可达82%，平均准确度可达96%左右。

关键词：状态变量；网络协议软件；程序分析技术；网络安全
https://doi.org/10.1631/FITEE.2200275