链滴

程序分析介绍

作者：Hanseltu
原文链接：https://ld246.com/article/1552745972037
来源网站：链滴

原文链接 程序分析介绍

课程背景

随着用户对软件的需求越来越高，大多数程序变得越来越大，越来越复杂，越来越难分析。对于一般软件，会存在以下几个问题：

<center><img src="https://b3logfile.com/file/2019/03/problems-4ea92906.png" width="70
" height="70%" /></center>

对于研究者来说，程序也是数据，我们可以使用工具来对其进行：

● 分析

<center> </center>

● 转换

<center> <img src="https://b3logfile.com/file/2019/03/transform-c01b2054.png" width="7
%" height=256 /> </center>

● 合成

<center><img src="https://b3logfile.com/file/2019/03/synthesize-f3583b0e.png" width="70
" height=256 /> </center>

综上，程序就像普通的数据一样，只是数据一种存在的形式。对程序的表示，分析，转换，合成等技就叫做程序分析技术（program analysis）。

课程目标

使用程序分析技术解决实际应用场景中出现的问题，程序分析的任务包括：

● 剖析（Profiling）

Speed, Potential Concurrency, Memory.

● 测试（Testing）

More effective tests. Bridge testing & verification.

● 调试（Debugging）

Explaining or locating the causes of bugs.

● 并发（Concurrency）

How to explain race conditions?

Atomicity violations?

How to find 'Heisenbugs'?

● 安全（Security）

How to find vulnerabilities before attackers?

- 验证（Verification）

How to prove the absence of behaviors?

指导性问题

- These problems are impossible to precisely solve in general. What are the compromises?
  - What cornercases make them fail?
  - Why do these cornercases exist?
- How do authors present their work? Why?
  - What is highlighted? What is hidden?
  - How is it evaluated?

课程结构

<center> </center>

>> 回到课程主目录