操作系统设计及实践

《操作系统原理》配套实验

信安系操作系统课程组

2022年11月

武漢大学

操作系统设计实验系列（十二）

自我OS的安全性分析与可信防御

武漢大学

实验目标

1. 结合所学的软件安全知识以及OS知识，分析掌握OS设计中潜在的安全问题
2. 学习与理解可信动态度量的基本思想与基本实现手段。

实验内容

1. 自我OS安全分析
   - ① 分析提示：可执行文件的篡改、内存破坏漏洞、权限绕过等
   - ② POC实现：
     - ① 编写一个C程序，该程序查找OS中的可执行文件，对可执行文件添加额外的代码。
     - ② 编写一个程序，可对存在内存破坏漏洞的代码进行缓冲区溢出，控制返回地址到指定的位置

实验内容

2. 可信防护

① 静态度量：

- 对你的OS进行扩充，编写一个程序模块，该程序模块能够在，当OS加载可执行文件时，对该可执行文件进行完整性校验，并进行比对。
- 完整性校验的算法，可采用简单的奇偶校验算法。
- 思考：
  - 这样的度量，是否能够抵御对可执行文件的篡改？
  - 完整性校验算法，使用奇偶校验算法，是否存在什么问题？
  - 完整性校验值应该存在哪里？

实验内容

2. 可信防护

② 动态度量：

- 对你的OS进行扩充，编写一个自动化的触发程序
- 触发时，读取当前运行的进程的内存布局进行，并解析堆栈结构，检查堆栈返回地址是否合法
- 思考：
  - 如何理解“合法”的概念？
  - 你的实现能否抵御POC实现中，第二个攻击？
  - 这种度量方法的效率如何，存在什么额外的安全问题？

实验内容

2. 可信防护

③ 感知与体系化防护（选做）：

- 对你的OS进行扩充，探索体系化防护思路。明确攻击平面有哪些?并考虑相应防护。例如：
  - 内存破坏：借鉴软件安全中的方法，试试比如地址空间布局随机化、Canary、页面的权限管理？
  - 系统调用的滥用：是否可以扩展一套系统调用的hook机制，并加以分析
  - 数据窃取：提供基于文件系统、或者内存的加密机制？
  - .....
  - 可以发挥你的想象力，在这个demo系统上探索。

谢　谢！