第 1 讲：Advanced OS Overview

第五节：Tendency of OS – Reliability

陈渝

清华大学计算机系

yuchen@tsinghua.edu.cn

2020 年 2 月 15 日

Tendency

- Performance
- **Reliability**
- Correctness

Definition

Reliability: from IEEE definition

The ability of a system or component to perform its required functions under stated conditions for a specified period of time

Definition

Reliability: from IEEE definition

The ability of a system or component to perform its required functions under stated conditions for a specified period of time

- Usually stronger than simply availability: means that the system is not only “up” , but also working correctly
- Includes availability, **security, fault tolerance**/durability
- Must make sure data survives when system crashes, disk crashes, etc

History of Security Problem

- Originally, there was no security/safety problem
- Later, there was a problem, but nobody cared
- Now, there are increasing problems, and people are beginning to care

Threat Analysis

- What are we trying to protect? (and why?)

Threat Analysis

- What are we trying to protect? (and why?)
- What are the vulnerabilities of those assets?

Threat Analysis

- What are we trying to protect? (and why?)
- What are the vulnerabilities of those assets?
- Who might （accidently） exploit a vulnerability?

Threat Analysis

- What are we trying to protect? (and why?)
- What are the vulnerabilities of those assets?
- Who might （accidently） exploit a vulnerability?
- How can we prevent a specific threat?

Threat Analysis

- What are we trying to protect? (and why?)
- What are the vulnerabilities of those assets?
- Who might （accidently） exploit a vulnerability?
- How can we prevent a specific threat?
- How much is it worth to us to prevent it?

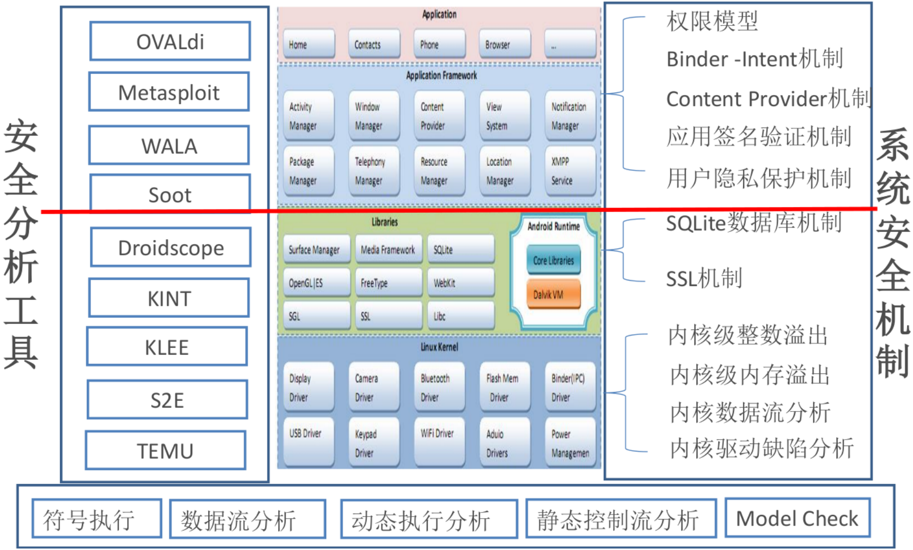
Threat Analysis

- What are we trying to protect? (and why?)
- What are the vulnerabilities of those assets?
- Who might （accidently） exploit a vulnerability?
- How can we prevent a specific threat?
- How much is it worth to us to prevent it?

The Core Technical Problem

- Controlling access to machine and data resources
- Controlling the way access rights are passed from holder to holder
  - person to person
  - program to program
- Preventing maliciousness and errors from subverting the controls

System Security Technology



安全分析工具

OVALdi

Metasploit

WALA

Soot

Droidscope

KINT

KLEE

S2E

TEMU

权限模型

Binder -Intent机制

Content Provider机制

应用签名验证机制

用户隐私保护机制

SQLite数据库机制

SSL机制

内核级整数溢出

内核级内存溢出

内核数据流分析

内核驱动缺陷分析

系统安全机制

符号执行

数据流分析

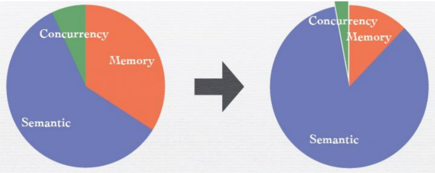
动态执行分析

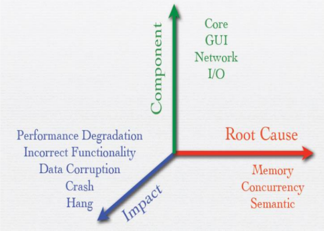
静态控制流分析

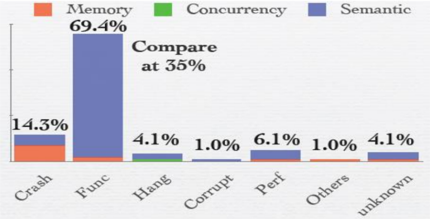
Model Check

Current Status

- 对当前 Android 漏洞的理解
    - Sematic Vulnerability 越来越多
    - 数据泄漏漏洞的威胁越来越大

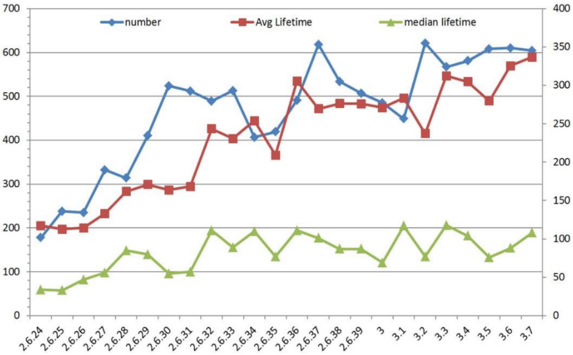


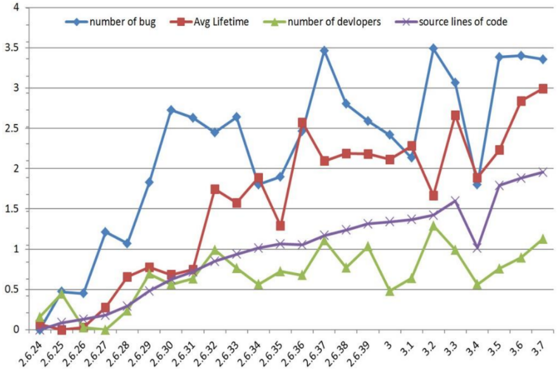




Current Status

- 对当前 Linux Kernel 漏洞的理解
  - Linux 漏洞有扩大化的趋势
  - 但发现 Linux 漏洞难度加大


number
Avg Lifetime
median lifetime


number of bug
Avg Lifetime
number of devlopers
source lines of code