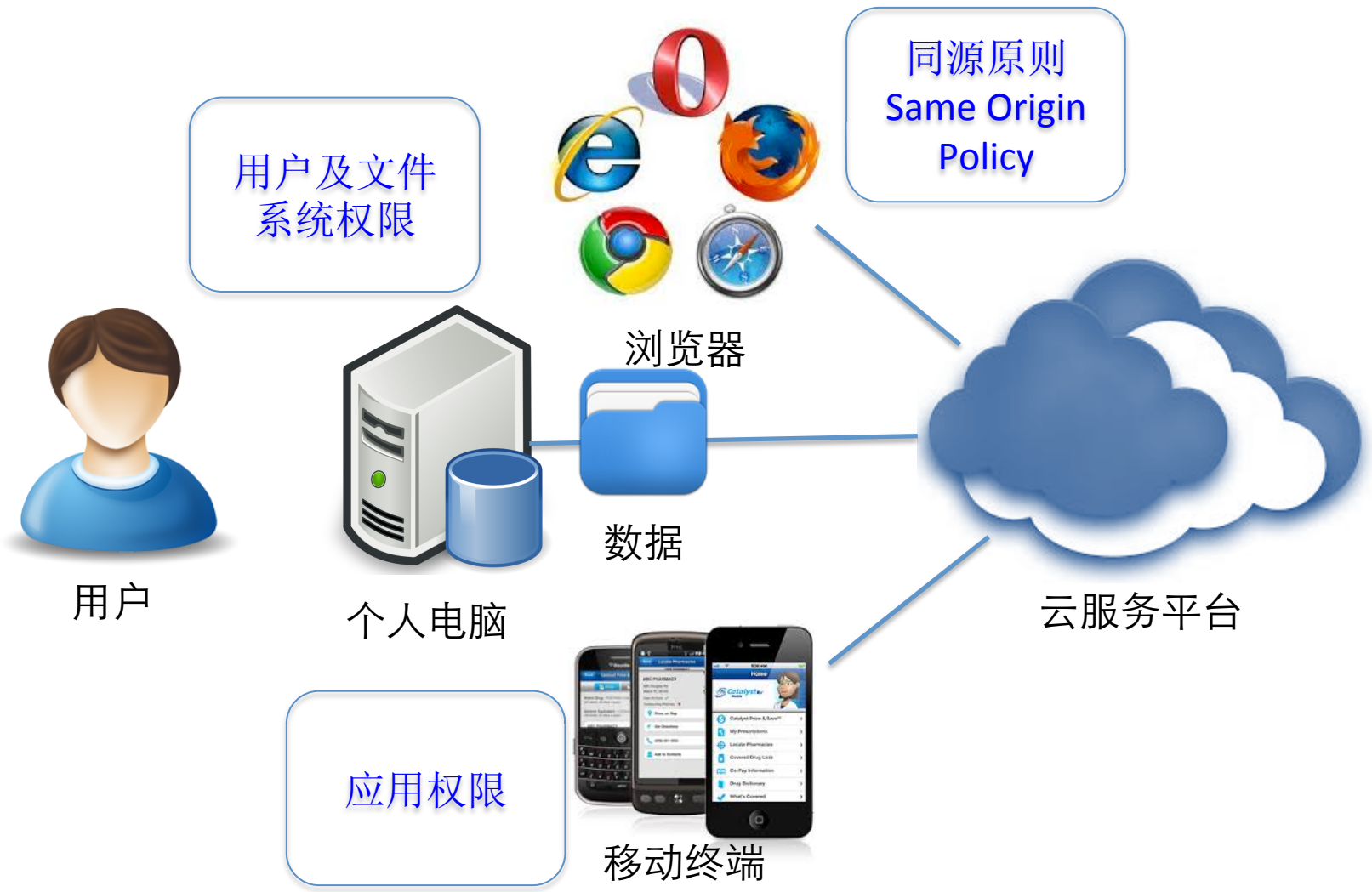
Web平台和移动平台上面向数据的保护机制

梁振凯

新加坡国立大学

日趋复杂的计算平台


同源原则
Same Origin
Policy
用户及文件
系统权限
浏览器
数据
用户
个人电脑
云服务平台
应用权限
移动终端

新的安全挑战

异构的系统平台

- 多源的操作系统和应用程序

开放的运行环境

- 共存的恶意代码

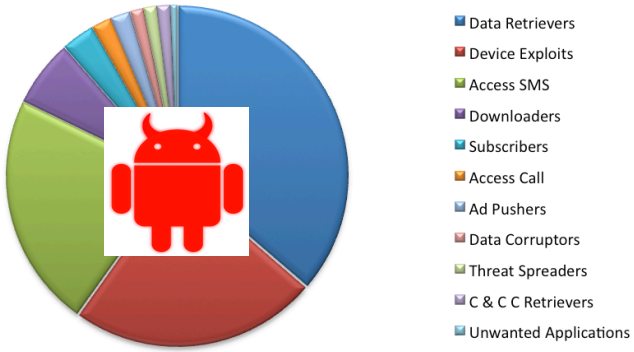
跨平台数据推送

- 数据在不同平台中存在多个副本

安全问题实例

- 浏览器：第三方代码注入
  - 基本安全机制：基于源站点的隔离
  - 安全问题：跨站点脚本注入（XSS），恶意浏览器扩展
    - 注入的JavaScript代码能够以用户权限访问用户的数据

- 移动设备：恶意的程序和系统
  - 基本安全机制：基于程序的隔离
  - 安全问题：重新打包的程序，系统级rootkit
    - 用户的数据对恶意代码完全开放



现有安全机制的不足

- 缺乏统一数据的保护规则
  - 不同的保护机制
  - 不同的用户概念
- 数据过度暴露给无关代码
  - 粗粒度的隔离机制
  - 可信计算基（TCB）代码量庞大

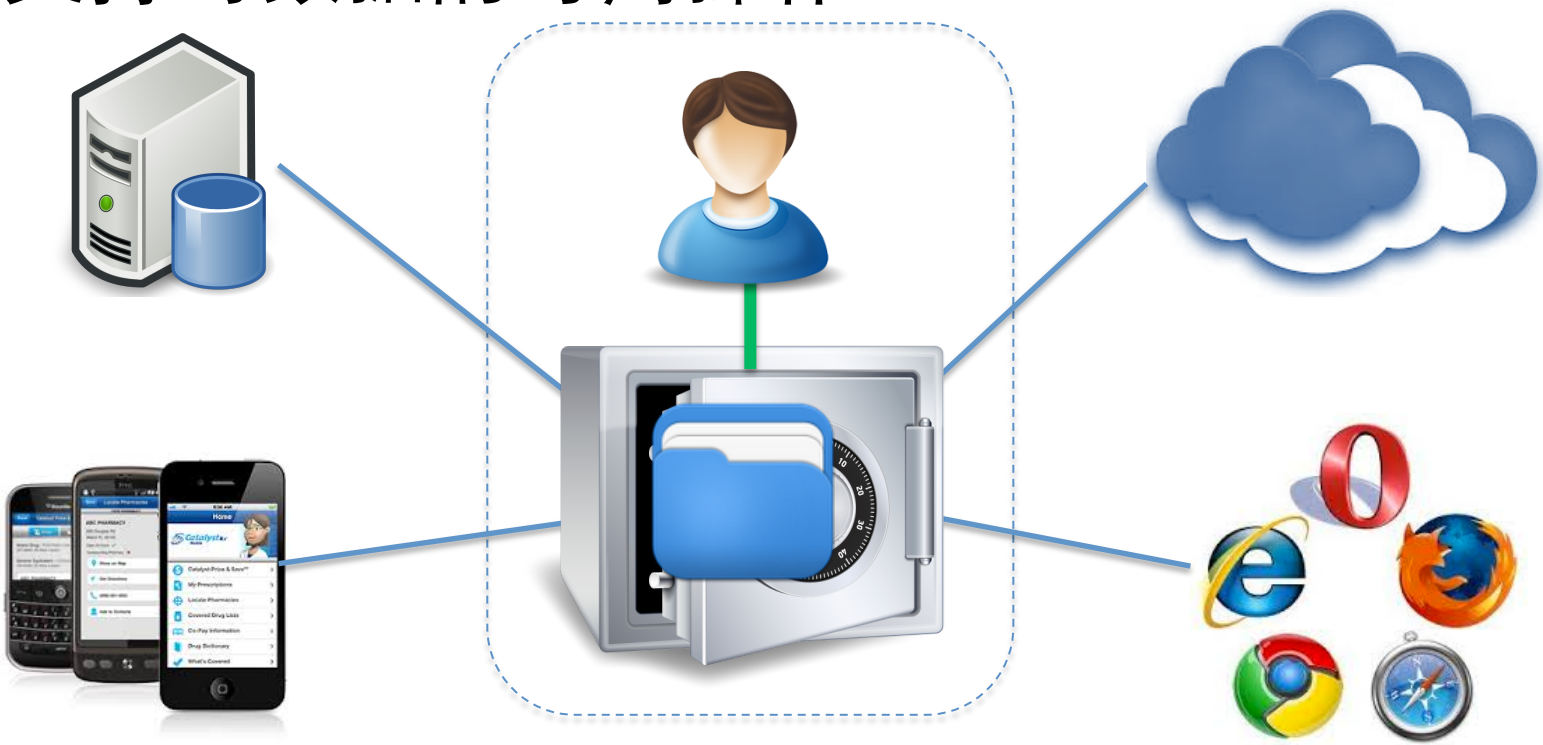
数据安全依赖于处理平台
所支持的安全机制

用户

数据

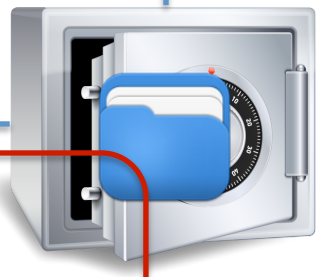
面向数据的保护机制

- 统一的用户概念和安全策略
- 独立于运行平台的安全保证
- 支持对数据的可用操作



核心机制

用户签名和验证

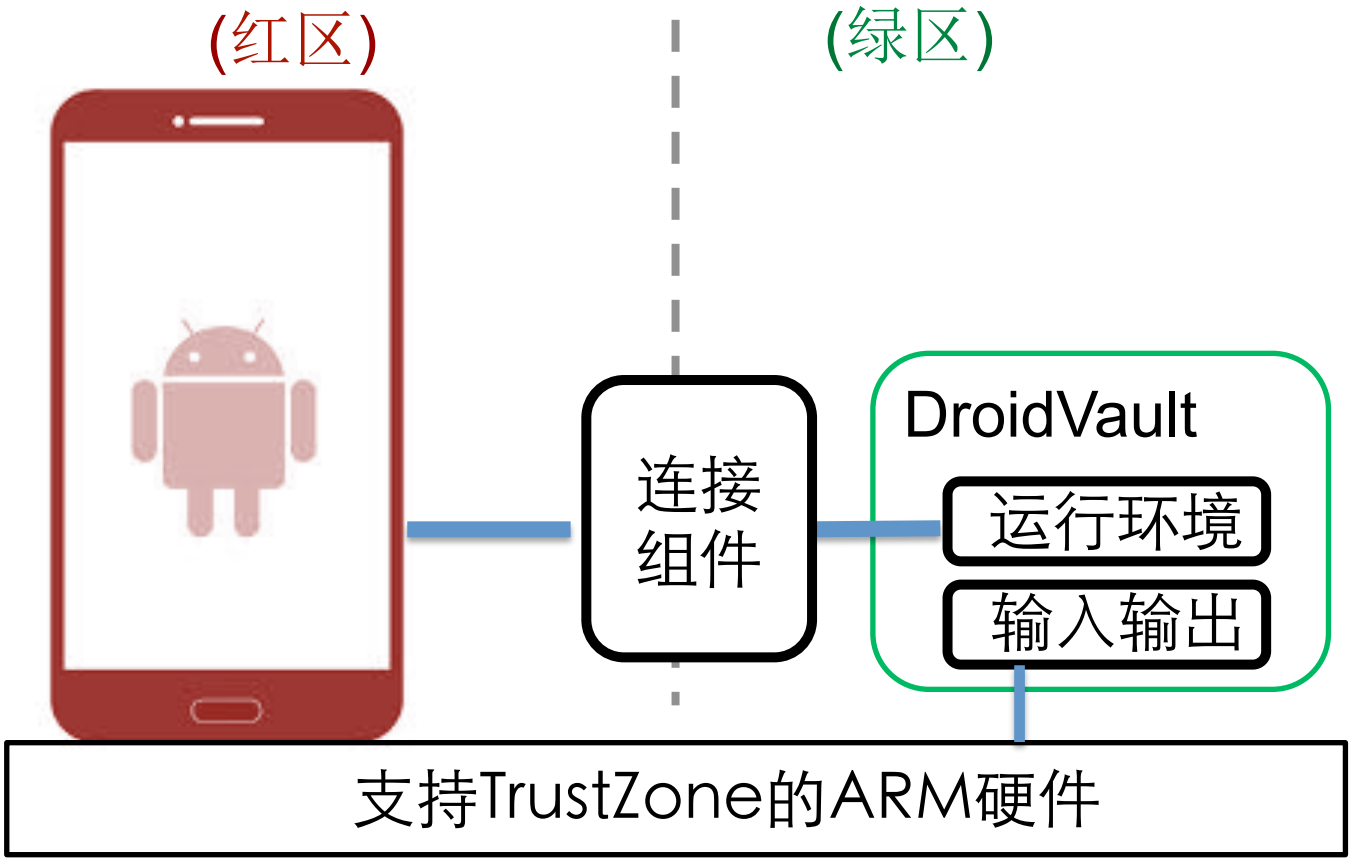


数据加密

数据操作

- 安全存储
- 安全通信
- 安全输入输出
- 用户认证的操作

Android平台：DroidVault

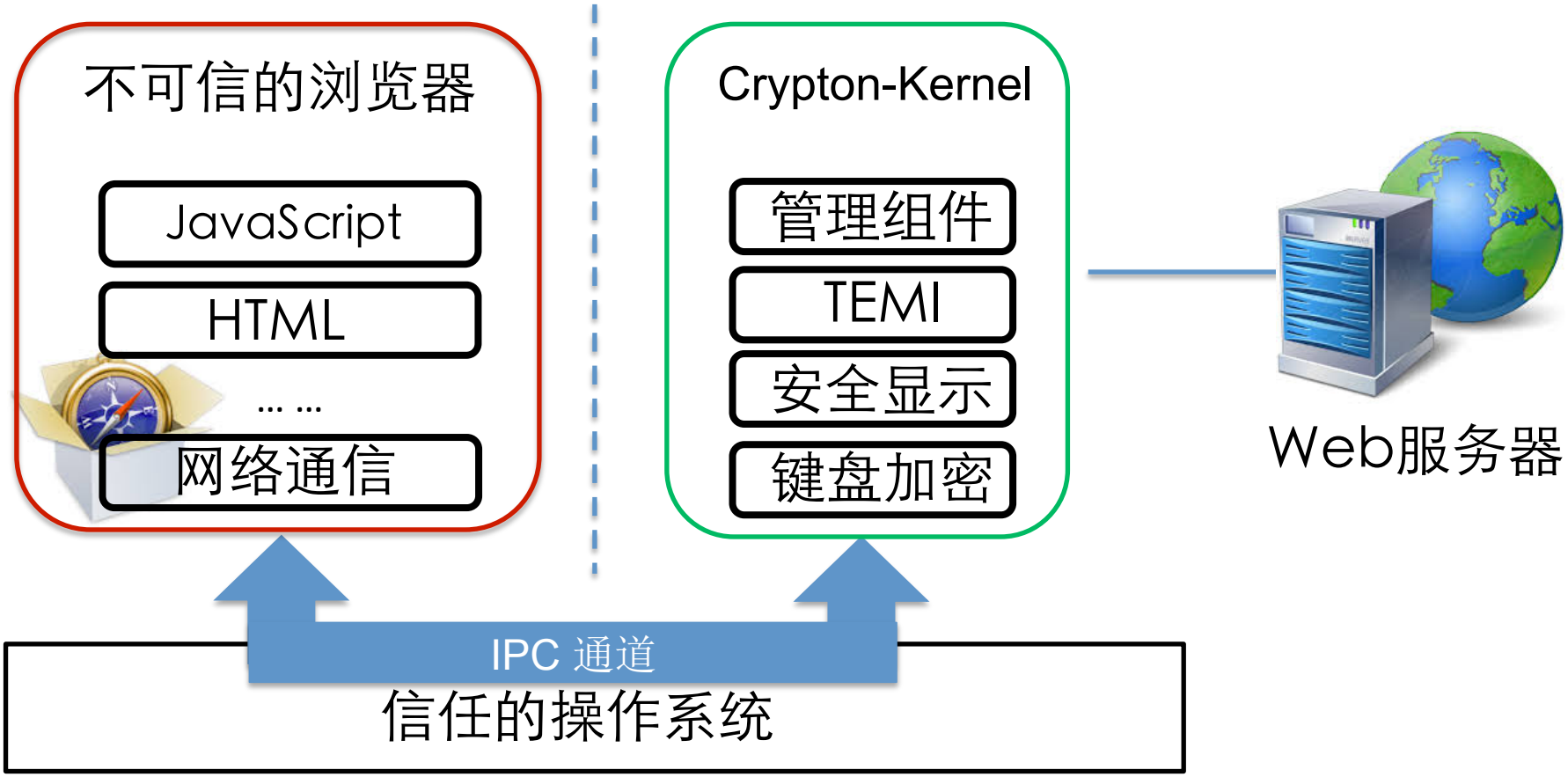


- 基于ARM处理器的TrustZone机制，把硬件平台划分为红区和绿区。
- 在绿区中实现微型数据保护的操作环境。

DroidVault系统实现

- 软硬件组件
  - Freescale i.MX53 QSB
  - Open Virtualization, PolarSSL
- 应用：云平台文件管理器
  - 安全环境中基于SSL登录
  - 安全文件传输和存储
  - 简单文件处理

Web平台： Crypton



- 基于Webkit-GTK的实现
- 20个开源Web应用的兼容性测试（<1%代码修改）

研究展望

- 面向数据的保护机制
  - 由简单的可信任环境保障复杂环境中数据安全
  - 丰富的功能支持
- 异构计算平台中的安全
  - 由不可信组件构造安全的运行平台
  - 漏洞检测，组件加固，系统验证

谢谢指正！

梁振凯 liangzk@comp.nus.edu.sg
http://www.comp.nus.edu.sg/~liangzk