软件与系统安全研究

Software Security Research in Progress

2019-10

研究方向

- 各平台上的多程序语言代码的安全分析与防护
  - 平台：服务器、个人计算机、移动智能设备、嵌入式和工控设备
  - 架构：x86/64、ARM/ARM64、MIPS、RISC-V
  - 语言：汇编、C、C++、Java、Python、Obj-C、Solidity
- 挖掘软件中存在的安全问题
  - 内存破坏漏洞、软件逻辑错误、配置错误导致的风险
  - 身份认证不当、协议保护缺失、密码算法误用
  - 设计正确、实现上不一致导致的安全问题
- 软件安全问题的自动化修复
  - 基于已有修复方案的迁移
  - 对具有相似模式的漏洞代码的自动化修复

研究成果

1. 软件自动化安全分析与软件漏洞修复

2. 移动智能终端安全

3. 智能家居与嵌入式设备安全

4. 密码算法与密码协议的误用分析

基于内存挤压的漏洞利用技术

- 通过消耗物理内存（内存挤压），绕过系统针对use-after-free（UAF）漏洞的防御机制（ASLR），完成通用攻击
  - CVE-2015-3636：针对Linux内核ping socket UAF的exploit
  - 2015年CCS会议论文，并获2017上海市计算机学会信息安全最佳论文奖
  - 2015安全漏洞最高奖**Pwnie Award最佳提权漏洞提名**（全球仅4项）

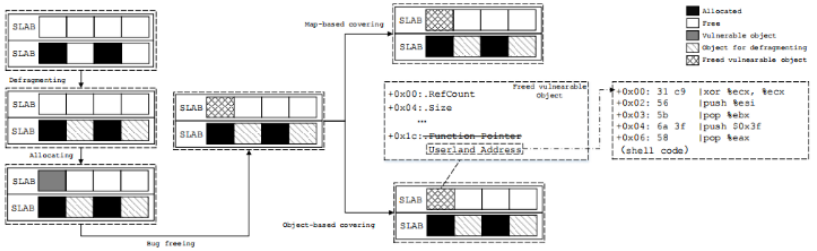
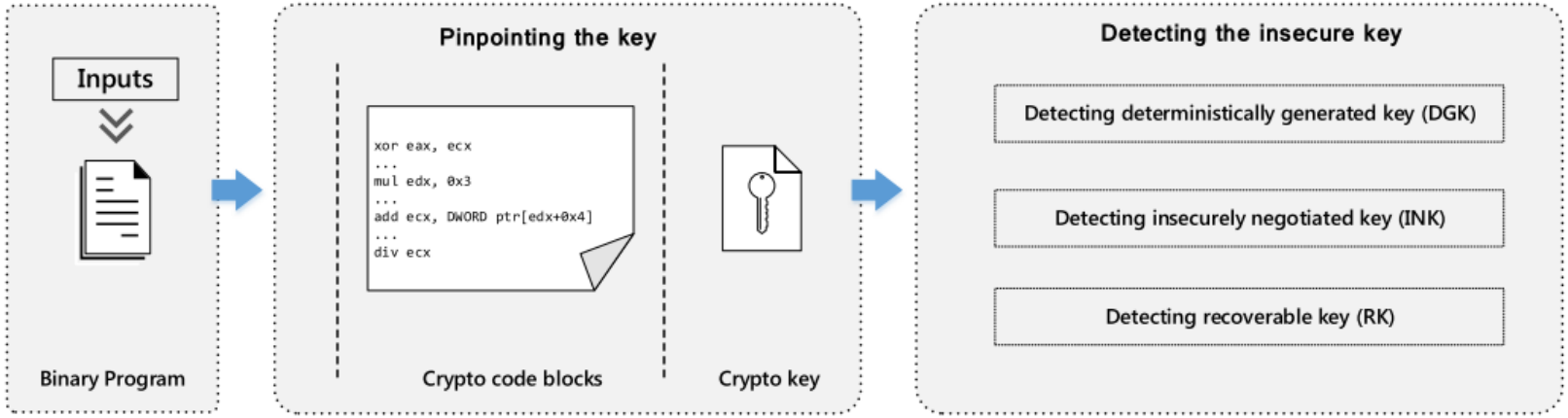


Figure 1: Memory Collision Attack

二进制代码中的密钥安全分析

- 检测Windows、Linux和macOS上的x86/64二进制代码中不安全的密钥
- 针对10个密码学算法库和15个包含密码算法的工具软件，发现其中22个程序不安全地使用了密钥！
- 2018年CCS会议论文，首个密码算法无关的不安全密钥检测研究
- 2019年网络安全研究国际论坛（Inforsec） 主题演讲



自动化软件漏洞修复技术

- 针对操作系统内核和系统库文件的二进制代码中存在的软件漏洞，无需源代码即可进行修复
  - 利用二进制重写技术对漏洞进行修复
  - 巧妙利用原有漏洞的脆弱性，绕过系统的保护机制，重写内核相关代码
  - 典型案例：对存在多项限制措施（防修改、防重写）三星S6手机的漏洞修复
  - 2017年ICSME会议学术论文，已被Usenix Security、NDSS、RAID、Euro S&P论文引用!

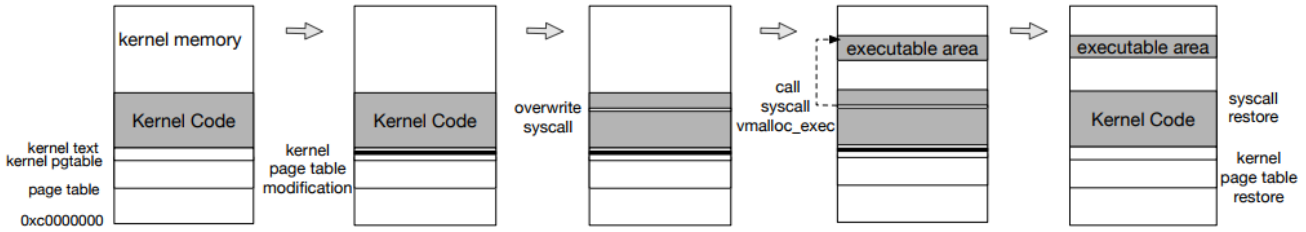
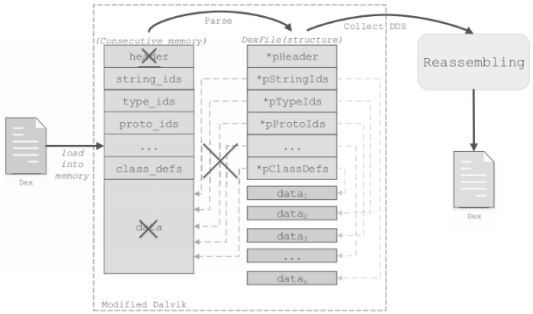


Fig. 3. allocate an executable kernel memory region

Android App的代码通用脱壳技术

- 基于代码重组的Android APP脱壳，对抗10种主流代码保护方案
  - 分析了阿里聚安全，百度安全，360安全，梆梆加固，爱加密等10个主流厂商的加固方案
  - 2015 RAID 国际学术会议学术论文，后续45次引用，该领域开创性研究
  - 2015年乌云峰会主题演讲



360加固保 jiagu.360.cn

爱加密

梆梆安全 BANGCLE

应用加固

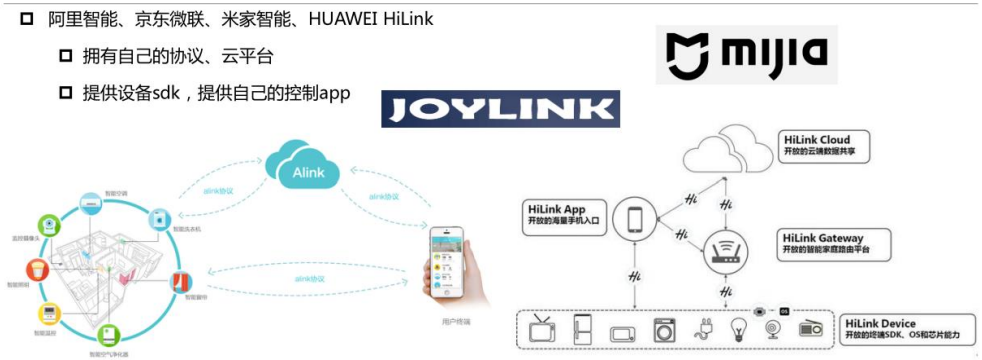
阿里聚安全 应用更安全，用户更安心！

移动支付安全研究

- 第三方移动支付安全研究
  - 发现了**微信、支付宝、银联支付、百度钱包**等4种移动支付SDK的安全漏洞，解决了991款移动应用的支付安全问题，提出支付防护方案
  - 2016年我们发现了任意金额消费、任意指纹支付（**华为 Mate8 TEE**）等高危安全风险
  - 设计开发了移动支付安全的系统性防护方案（NDSS'17 学术论文）

智能设备和嵌入式安全分析

- 2018 互联网安全领袖峰会主题演讲
  - 《易伪造的数字钥匙——智能门锁Token安全性分析与防护》
- 2018 DEF CON 神州安全大会主题演讲
  - 《路上Wi-Fi欲断魂：攻击SmartCfg无线配网方案》
- 2017 中国互联网安全大会（ISC）主题演讲
  - 《智能家居平台中的隐私与安全问题》



密码协议的安全分析

- SSL/TLS协议安全问题：协议降级攻击、协议证书问题
  - 发现了12306、苏宁易购存在的协议降级攻击并成功复现（需要分解512比特RSA）
  - 2016乌云峰会安全演讲
- OAuth协议安全问题：OAuth协议中的认证和授权安全问题的研究
  - 在ACSAC 2015、2016 学术会议上发表论文
  - 360互联网安全大会主题演讲

Heartbleed攻击

POODLE攻击

现实软件中的密码学误用

- 首个iOS平台上的大规模密码学误用检测系统iCryptoTracer
  - NSS 2014学术论文，已获得25次引用
- 首个Android平台Native代码密码学误用分析系统NativeSpeaker
  - Inscrypt 2018学术论文，被RAID 2019论文引用
- 针对Android平台私有OpenVPN实现密码学误用的攻击
  - 腾讯安全探索论坛主题演讲
  - CANS 2018学术会议论文