# 目录

# 信息安全概览

- 最新版本：`v0.2`
- 更新时间：`20200731`

# 简介

边学习信息安全技术，边总结技术教程。已整理出宏观的各个方面的安全的分类和概念。以及基本的计算机安全、移动端安全、物联网安全等细节内容。

# 源码+浏览+下载

本书的各种源码、在线浏览地址、多种格式文件下载如下：

## Gitbook源码

- crifan/information_security_overview: 信息安全概览

## 如何使用此Gitbook源码去生成发布为电子书

详见：crifan/gitbook_template: demo how to use crifan gitbook template and demo

## 在线浏览

- 信息安全概览 book.crifan.com
- 信息安全概览 crifan.github.io

## 离线下载阅读

- 信息安全概览 PDF
- 信息安全概览 ePub
- 信息安全概览 Mobi

# 版权说明



# 鸣谢

感谢我的老婆**陈雪**的包容理解和悉心照料，才使得我 `crifan` 有更多精力去专注技术专研和整理归纳出这些电子书和技术教程，特此鸣谢。

# 概览

## 背景

先说说写这个教程的背景：

- 之前已写过 安卓安全和破解 的教程
  - https://github.com/crifan/android_app_security_crack
    - 目前点赞不少 500+个star
    - 看来大家比较关注这个领域
- 自己计划从事 `计算机安全领域`
  - 之前是小白，没这方面的经验
  - 打算边自学，边总结，总结到这个教程中
    - 供自己和他人参考

## 信息安全技术概览

此处对于信息安全相关技术进行概述。

信息安全技术概念包含内容较多，且涉及维度较广，下面以不同维度来阐述，常见分类和对应内容。

- 信息安全
  - 根据不 `同端` = `目标` = `设备` 分
    - `Web端` ： `网络安全` = `Web安全` = `互联网安全`
    - `PC端` ： `计算机安全`
      - 包含
        - `Windows`
        - `Mac`
        - `Linux`
    - `移动端` ： `移动安全`
      - 包含
        - `Android`
        - `iOS`
    - `IoT端` ： `物联网安全`
  - 广义的信息安全
    - 子领域=特殊领域
      - `信息存储安全`
        - 典型应用场景：指纹、虹膜、信用卡PIN码等
        - 包含
          - 硬件
            - `TrustZone`
          - 软件
            - `OP-TEE`

# 安全通用知识

此处整理各方面的安全的基础和通用的知识。

# 破解 vs 开发

- **破解**：属于 `逆向`
- **开发**：属于 `正向`

# 常见问题

## 问：做安全的破解的，是否一定要会开发？

- 答：不一定。但最好会。
  - 做安全破解的，会开发，属于加分项。
  - 原因也很简单
    - 就像：做逆向破解的就像小偷去你别家偷东西
    - 肯定没有，作为正向开发，作为开发商建造房子的你，对房子内部构造更熟悉，更容易找到突破口，找到可能的漏洞，并充分利用漏洞去实现自己的攻击。

# 设备端安全

和Web网络相对应的，可以统称为 设备端的安全。

主要包括：

- PC端
  - Windows
  - Mac
  - Linux
- 移动端
  - Android
  - iOS
- IoT=物联网设备

下面根据不同维度详细介绍。

# 可执行文件 逆向工程 工具

- `Windows` 的 `PE` 格式的 `exe文件`
  - `OllyDBG`
  - `IDA PRO`
    - 二进制分析
  - `Hiew`
    - 反汇编 + 16进制编辑器
    - 命令行，无GUI
- `Linux` 的 `ELF` 格式的文件
  - `GDB`
  - `IDA PRO`
  - `Hopper`
    - Disassembler + Pseudo C decompiler
  - `Evan's debugger`
    - Linux中类似于OllyDBG的工具
  - `Insight`
    - GDB的GUI
    - 有点过时了
- `Mac` 的 `MACH-O` 格式的文件
  - `Hopper`
  - `IDA PRO`
  - `LLDB`
  - `MachOView`
- `Android` 的 `dex` 格式的文件（apk文件内的）
  - `APK TOOL`
    - Disassembler and Assembler (SMALI)
  - `JEB`
    - Android disassembler (SMALI) and decompiler (JAVA)
  - IDA PRO

- `iOS` 的可执行文件
  - `IDA Pro`
  - `Hopper`
  - `otool`

TODO：

【未解决】Mac中有哪些常用的破解逆向方面的工具软件

# 计算机安全

- PC端：计算机安全
  - 多平台：
    - IDA
    - radare2
  - Windows
    - Windows安全
      - 调试工具
        - `OD = OllyDbg = Olly DBG`
        - `WinDBG`
        - `LLDB`
  - Mac
    - 工具
      - `Hopper Disassemble`
  - Linux
    - `LLDB`
    - `GDB`
- 对比
  - 静态分析：`IDA`
    - 支持插件：
      - 最强大的：`Hex-rays`
        - 把汇编语言转换成C语言伪代码
  - 动态调试-》调试器：`WinDGB` 、 `OllyDBG`

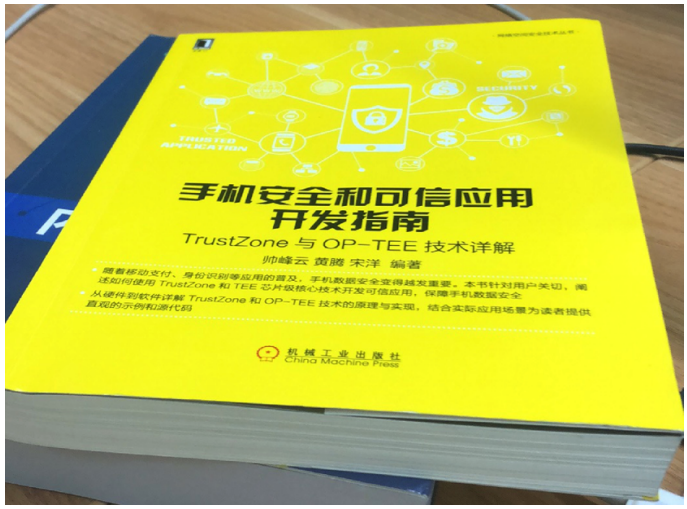
# 移动安全

- 移动端：移动设备安全
  - Android
    - Apk逆向工具
      - Apktool
      - jd-gui
      - dex2jar
    - apk反编译
      - apk
        - 脱壳
        - 加壳
      - Smali/Baksmali代码
    - Android
      - Hook技术
        - Xposed
      - 虚拟化技术
        - VirtualApp
        - DroidPlugin
  - iOS

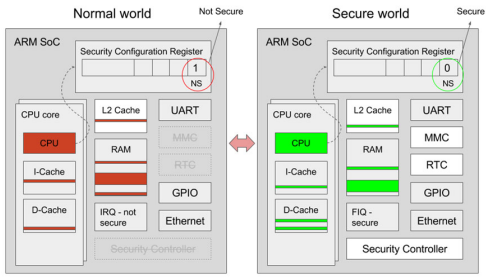
# 物联网安全

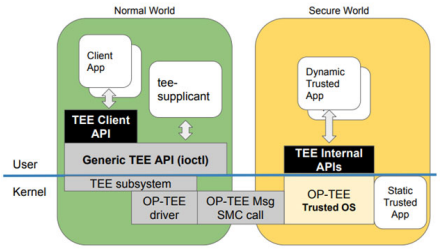
- IoT端：物联网安全

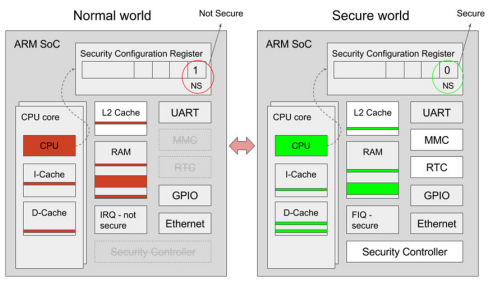
# 信息存储安全

- 信息存储安全
  - 应用场景和领域
    - 生物特征数据存储
      - 指纹
      - 虹膜
    - 信用卡PIN码（保存）
    - 私有密码（存储）
    - 客户数据（存储）
    - 受 `DRM` = `Digital Rights Management` = `数字版权管理` 保护的媒体
  - 相关书籍
    - 《手机安全和可信应用开发指南》 TrustZone与OP-TEE技术详解
    - 
      
  - 相关技术
    - 硬件层面
      - `Trust-Zone`
        - ARM
          - 提出了TrustZone技术
            - 为了确保数据安全
            - 用一根 `安全总线` （称为 `NS` 位）来判断当前处于 `secure world` 还是 `non-secure world` 状态
              - 状态的切换由 `ATF` = `ARM Trusted Firmware` 来完成
    - 软件层面
      - `TEE` = `OP-TEE`
        - 名称
          - `TEE` = `Trusted Execution Environment` = `信任执行环境` = `可信任执行环境`
          - `OP-TEE` = `Open Portable Trusted Execution Environment` = `Open-Source Portable Trusted Execution Environment` = `开放可移植的可信任执行环境`
        - 一句话描述
          - 基于TrustZone技术搭建的安全执行环境

        - designed as companion to a non-secure Linux kernel running on Arm
            - 注：Cortex-A cores using the TrustZone technology
- 用途=目的=为什么
    - 为了更安全
        - 处理那些需要和安全密切相关的、需要保密处理的信息
- 历史
    - 最早是ST-Ericsson开发的
        - http://www.stericsson.com/
    - 2013年，ST-Ericsson实现了兼容GlobalPlatform
        - https://globalplatform.org/
    - 2013年之后，ST和Ericsson分开了
    - 现在TEE属于STMicroelectronics
        - https://www.st.com/content/st_com/en.html
    - 2013年后期，Linaro成立了SWG=Security Working Group=安全工作组
        - 其最重要的任务之一就是继续开发TEE
    - 在开源TEE之前，花了很多个月去把之前部分私有模块，换成开源实现
        - 包括：密码库, 安全监控, 编译系统及其他
    - 2014-06-12，TEE开源了，叫做OP-TEE
        - 目前现状主要是：
            - 项目属于STMicroelectronics
            - 但是Linaro和STMicroelectronics联合在开发
    - 2015年，项目所有权从STMicroelectronics转给Linaro了
- 资料
    - 官网
        - https://www.op-tee.org
    - GitHub
        - OP-TEE/optee_os: Trusted side of the TEE
            - https://github.com/OP-TEE/optee_os
    - 技术文档
        - OP-TEE Documentation — OP-TEE documentation documentation
            - http://optee.readthedocs.io
- 主要设计目标
    - Isolation
        - the TEE provides isolation from the non-secure OS and protects the loaded Trusted Applications (TAs) from each other using underlying hardware support,
    - Small footprint
        - the TEE should remain small enough to reside in a reasonable amount of on-chip memory as found on Arm based systems,

- Portability
  - the TEE aims at being easily pluggable to different architectures and available HW and has to support various setups such as multiple client OSes or multiple TEEs.
- `OP-TEE` 包含内容
  - `Secure world` OS= `optee_os`
    - 现有实现：
      - `OP-TEE OS`，`Trusty`，高通的 `QSEE`，`SierraTEE`
        - 注：所有方案的外部接口都会遵循 `GP` = `Global Platform` 标准
    - 对比：Normal world os
      - 普通操作系统：Linux、Android等
    - 问：各家厂商和组织的 `TEE OS` 到底有何区别?
      - 答：`TA` 的添加和加载时的校验有所区别
    - 系统架构
      - 

      - 

      - 

    - 相关概念
      - `TA` = `Trusted Application` =可信应用
      - `CA` = `Client Application` =客户端应用
    - 原理
      - 产品开发团队负责开发一个运行在 `Linux` 上的 `CA` 和一个运行在 `OP-TEE` 上的 `TA`
      - `CA` 使用 `TEE client API` 与 `TA` 通信，并且从 `TA` 获取安全服务
      - `CA` 和 `TA` 使用 `共享内存` 进行通信

        - 运行机制
            - 当处于 `secure world` 状态，那么就会执行 `TEE OS` 部分的代码
            - 当处于 `non-secure world` 状态时,就执行 `linux kernel` 部分的代码
        - `Normal world` client= `optee_client`
        - test suite = `optee_test/xtest`
        - linux驱动
    - 常见问题
        - Linux内核
            - Linux内核能直接访问TEE部分的资源吗?
                - Linux kernel不能直接访问TEE部分的资源
            - Linux 内核如何才能访问TEE部分的资源呢?
                - Linux kernel能通过特定的 `TA` 和 `CA` 来访问TEE部分特定的资源

# 附录

下面列出相关参考资料。

# 资料和文档

## 安全领域相关论坛

- 常见安全相关网站
  - t00ls
    - 简介
      - 十年民间网络安全老牌社区，聚合安全领域最优秀的人群，低调研究潜心学习讨论各类网络安全知识，为推动中国网络安全进步与技术创新贡献力量！
      - 当前国内为数不多的民间网络信息安全研究团队之一
  - wooyun=乌云
    - 最新：已关闭
    - 简介
      - 一个位于中国大陆的于企业与安全研究人员（白帽子）之间的安全漏洞报告平台，并提供最新的研究资讯。
      - 2016年7月20日凌晨，乌云官网突然关闭，仅显示一张“升级通告”的图片，并附言 “与其听信谣言，不如相信乌云”。据外界推测可能是内部整顿
      - 有多方消息表示多名乌云高管被警方带走，但同时也有人辟谣称是谣言。截至2020年3月，网站依仅展示升级公告。
  - freebuf
    - 简介：国内领先的互联网安全新媒体，同时也是爱好者们交流与分享安全技术的社区。
    - 官网
      - FreeBuf互联网安全新媒体平台
      - https://www.freebuf.com
  - 安全客
    - 简介：安全客 - 安全资讯平台
    - 网站：https://www.anquanke.com/
  - Seebug
    - 简介：一个权威的漏洞参考、分享与学习的安全漏洞平台，是国内权威的漏洞库，在国内和国际都享有知名度，于2006年上线。
    - 官网
      - 知道创宇 Seebug 漏洞平台 - 洞悉漏洞，让你掌握第一手漏洞情报！
      - https://www.seebug.org
  - exploit-db.com
    - 简介：一个面向全世界黑客的漏洞提交平台
    - 官网
      - Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers
      - https://www.exploit-db.com
  - 吾爱破解
    - 简介：吾爱破解论坛致力于软件安全与病毒分析的前沿，丰富的技术版块交相辉映，由无数热衷于软件加密解密及反病毒爱好者共同维护

        - 网站：https://52pojie.cn
    - Paper(知道创宇)
        - 简介：安全技术精粹
        - 网站：https://paper.seebug.org/
    - CTFWIKI
        - 简介：CTF Wiki
        - 网站：https://ctf-wiki.github.io/ctf-wiki/
    - CTFtime
        - 简介：Capture The Flag, CTF teams, CTF ratings, CTF archive, CTF writeups
        - 网站：https://ctftime.org/
    - 先知社区
        - 简介：先知社区，先知安全技术社区
        - 网站：https://xz.aliyun.com/

# 参考资料


- CTF.GS_CTF网站_CTF网址_CTF网址导航_CTF练习平台_CTF练习平台收集
- CTF大本营 - 网络安全竞赛服务平台-i春秋
- Hacker101 CTF
- CTFtime.org / All about CTF (Capture The Flag)
- optee开源项目的学习_fanguannan0706的专栏-CSDN博客_optee
- Open Portable Trusted Execution Environment - OP-TEE
- 什么是OPTEE-OS - 江召伟 - 博客园
- About OP-TEE — OP-TEE documentation documentation
- 【渗透测试工程师招聘】_暗泉信息招聘-BOSS直聘
- 漏洞利用 - 维基百科，自由的百科全书
- 漏洞 - 维基百科，自由的百科全书
- 计算机安全 - 维基百科，自由的百科全书
- 网络安全 - 维基百科，自由的百科全书
- 国内、国外网站安全渗透测试、漏洞扫描产品 | Venhow's Blog
- 渗透测试专业人员使用的11种工具 - FreeBuf互联网安全新媒体平台
- 谈谈我对逆向的一些认识 - 简书
- 「移动安全工程师招聘」_苏州极光无限信息...招聘-BOSS直聘
- 漏洞扫描原理——将主机扫描、端口扫描以及OS扫描、脆弱点扫描都统一放到了一起 - bonelee - 博客园
- 【知识科普】安全测试OWASP ZAP简介 - 知乎
- OWASP ZAP安全测试 - 简书
- 安全性测试：OWASP ZAP使用入门指南 - 哔哩哔哩
- Web安全测试-WebScarab工具介绍-云栖社区-阿里云