

目录

前言	1.1
安全概览	1.2
安全背景知识	1.3
编程语言	1.3.1
汇编语言	1.3.1.1
X86	1.3.1.1.1
ARM	1.3.1.1.2
体系架构	1.3.2
寄存器	1.3.2.1
X86	1.3.2.1.1
ARM	1.3.2.1.2
堆栈	1.3.2.2
安全通用知识	1.4
Web端安全	1.5
术语解释	1.5.1
常用工具	1.5.2
安全操作系统	1.5.2.1
Kali Linux	1.5.2.1.1
漏洞扫描类	1.5.2.2
AppScan	1.5.2.2.1
AWVS	1.5.2.2.2
Burp Suite	1.5.2.2.3
Cobalt Strike	1.5.2.2.4
Layer	1.5.2.2.5
Nessus	1.5.2.2.6
NetSparker	1.5.2.2.7
Nikto	1.5.2.2.8
N-Stalker	1.5.2.2.9
Whisker	1.5.2.2.10
Sn1per	1.5.2.2.11
WebScarab	1.5.2.2.12
Webinspect	1.5.2.2.13
Wikto	1.5.2.2.14
ZAP	1.5.2.2.15
端口扫描类	1.5.2.3

nmap	1.5.2.3.1
渗透测试类	1.5.2.4
Metasploit	1.5.2.4.1
模糊测试类	1.5.2.5
代码审计类	1.5.2.6
注入类	1.5.2.7
Sqlmap	1.5.2.7.1
组织和标准	1.5.3
OWASP	1.5.3.1
设备端安全	1.6
计算机安全	1.6.1
Windows	1.6.1.1
软件逆向	1.6.1.1.1
Mac	1.6.1.2
Linux	1.6.1.3
移动安全	1.6.2
物联网安全	1.6.3
特定设备安全	1.6.4
WiFi安全	1.6.4.1
Aircrack-ng	1.6.4.1.1
Wifiphisher	1.6.4.1.2
信息存储安全	1.7
其他安全相关	1.8
相关工具	1.8.1
抓包工具	1.8.1.1
Wireshark	1.8.1.1.1
破解密码	1.8.1.2
John the Ripper	1.8.1.2.1
Hashcat	1.8.1.2.2
Hydra	1.8.1.2.3
代理工具	1.8.1.3
附录	1.9
资料和文档	1.9.1
参考资料	1.9.2

信息安全概览

- 最新版本: v0.9
- 更新时间: 20200803

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

此电子书教程的全部内容，如无特别说明，均为本人原创和整理。其中部分内容参考自网络，均已备注了出处。如有发现侵犯您版权，请通过邮箱联系我 admin 艾特 [crifan.com](#)，我会尽快删除。谢谢合作。

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。

安全概览

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

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
 - 设备端
 - 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
 - 其他特定设备
 - WiFi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

安全背景知识

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-02 20:34:06

编程语言

- 编程语言种类

- 机器语言：用二进制编码表示每条指令，是计算机能直接识别和执行的语言。

- 原理：底层都是0和1的二进制数据
 - 注：理论上来说，程序员也可以写机器语言
 - 只不过太难写，以及没必要直接写，所以实际上没人直接写机器语言

- 汇编语言

- 实质和机器语言是相同的，都是直接对硬件操作，只不过指令采用英文缩写的标识符，更容易识别和记忆

- 组成

- 指令，伪指令，宏指令

- 逻辑

- 你（程序员）写汇编的字母（和要操作的数字等），汇编程序帮你把汇编的字母（和数字）翻译成0和1的二进制
 - 这样机器才能看懂，才能运行对应程序

- 高级语言

- 编写的程序不能直接被计算机识别，必须经过转换（目标代码即机器码）才能被执行

- 按照转换方式分类

- 解释类：边翻译边执行

- 编译类：先翻译再执行

- 常见语言

- C

- C语言的特点

- C语言允许直接访问物理地址，可以直接对硬件进行操作

- C语言程序代码质量高，程序执行效率高

- C语言使用范围大，可移植性好

- C++

- 由于：C++编译器优化程度太高

- 结果：世界上没有C++反编译器

- 也没有完美的C语言反编译器

- 很难做到完美

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-08-03 22:18:56

汇编语言

- 汇编
 - 汇编 = 汇编语言 = 汇编指令
 - 是什么
 - 汇编大多是指汇编语言，汇编程序
 - 把汇编语言翻译成机器语言的过程称为汇编
 - 汇编语言
 - 在汇编语言中，用符号代替机器语言的二进制码，就把机器语言变成了汇编语言
 - 是用助记符，符号和数字等来表示指令的程序设计语言，它与机器语言指令是一一对应的
 - 汇编程序
 - 用汇编语言编写的程序，机器不能直接识别。要由一种程序将汇编语言翻译成机器语言，这种起翻译作用的程序叫汇编程序。
 - 汇编程序是系统软件中语言处理的系统软件
 - 特点
 - 由于汇编更接近机器语言，能够直接对硬件进行操作，生成的程序与其他的语言相比具有更高的运行速度，占用更小的内存
 - 应用
 - 因此在一些对于时效性要求很高的程序，许多大型程序的核心模块以及工业控制方面大量应用
 - 种类
 - 有多少种不同内核的CPU，就有多少种汇编语言
 - 总结
 - 不同内核的CPU，必须有对应的汇编语言编译器将汇编语言编写的程序编译成对应CPU的机器语言代码，CPU才能正确识别和执行这些代码
 - 不同架构的CPU的汇编指令集并不相同
 - 不同的汇编程序有不同的汇编语言规定

通用知识

和逆向和破解相关的汇编语言的通用知识：

- 逆向中关键的指令：
 - `ldr` , `mov` , 读取指令，从地址读取数据到寄存器。
 - `str` , 保存指令，保存数据到寄存器。
 - `b` , 跳转指令，跳转到某个地址。
 - `cmp` , 比较指令，说明这里有分支。

X86汇编语言

- 常见X86汇编语言类型
 - ASM
 - MASM
 - TASM
 - OPTASM
 - 等

Intel 8086的汇编语言指令

- Intel 8086的指令
 - 概述
 - 117条基本指令
 - 6个功能组
 - 数据传送类指令
 - MOV/XCHG, PUSH/POP, LEA
 - 算数运算类指令
 - ADD/ADC/INC, SUB/SBB/DEC/CMP/NEG, MUL/IMUL, DIV/IDIV
 - 位操作类指令
 - AND/OR/XOR/NOT/TEST
 - 串操作类指令
 - 控制转移类指令
 - JMP/JCC/LOOP, CALL/RET, INT n
 - 处理机控制类指令
 - NOP
 - 其他
 - 伪指令

数据传送类指令

- 数据传送类指令
 - 概述：计算机中最基本，最重要的一种操作，传送指令也是最常用的一类指令
 - 作用：传送指令把数据从一个位置传送到另一个位置。
 - 特点：除标志寄存器传送指令外，均不影响标志位
 - 包含：`MOV XCHG PUSH POP LEA`
 - 传送指令`MOV`
 - 把一个字节或操作数从源地址传送至目的地址
 - 交换指令`XCHG`
 - 把两个地方的数据进行互换
 - 寄存器与寄存器之间对换数据
 - 寄存器与存储器之间对换数据
 - 不能在存储器与存储器之间对换数据
 - 进栈指令`PUSH`

- PUSH
 - Push r16/m16/seg 操作过程: 1. SP<-SP-2 2.SS:[SP]<-r16/m16
- POP
 - 出栈指令, 操作与PUSH相反
- 算数运算类指令
 - 概述: 四则运算计算机经常进行的一种操作
 - 作用: 实现二进制(十进制)数据的四则运算
 - 特点: 算术运算类指令往往对标志有影响
 - 建议
 - 掌握 ADD/ADC/INC , SUB/SBB/DEC/NEG/CMP
 - 熟悉 MUL/IMUL , DIV/IDIV
 - 理解 CBW/CWD , DAA/DAS , AAA/AAS/AAM/AAD
- 包含
 - 加法指令ADD
 - 功能: ADD指令将源与目的操作数相加, 结果送到目的操作数
 - ADD指令按状态标志的定义相应设置状态标志
 - 语法:
 - ADD reg, imm/reg/mem reg<-reg+imm/reg/mem
 - 带进位加法指令ADC
 - 功能: ADC指令将源与目的的操作数相加, 在加上进位CF标志, 结果送到目的操作数
 - ADC指令按状态标志的定义相应设置状态标志
 - 用途: ADC指令主要与ADD配合, 实现多精度加法运算
 - 语法:
 - ADD reg , imm/reg/mem
 - ADC mem , imm/reg
 - 增量指令INC
 - 功能: 对操作数加1(增量)
 - 不影响进位CF标志, 按定义设置其他状态标志
 - 语法:
 - INC reg/mem reg/mem<-reg/mem+1
 - 减法指令SUB
 - 功能: 将目的操作数减去源操作数, 结果送到目的操作数
 - 按照定义相应设置状态标志
 - 语法:
 - SUB reg , imm/reg/mem reg<-reg-imm/reg/mem
 - 带借位减法指令SBB
 - 功能: SBB指令将目的操作数减去源操作数, 在减去借位CF(进位), 结果送到目的操作数
 - 用途: SBB指令主要与SUB配合, 实现多精度减法运算

- 语法: SBB reg , imm/reg/mem reg<-reg-imm/reg/mem-CF
- 减量指令DEC
 - 功能: DEC指令对操作数减1 (减量)
 - 语法: DEC reg/mem reg/mem<-reg/mem-1
 - 说明: INC指令和DEC指令都是单操作数指令, 主要用于对计数器和地址指针的调整
- 求补指令NEG
 - 功能: NEG指令对操作数执行求补运算: 用0减去操作数, 然后结果返回操作数, 求补运算也可以表达成, 将操作数按位取反后加1
 - NEG指令对标志的影响与用0作减法的SUB指令一样
 - 语法: NEG reg/mem reg/mem<-0-reg/mem
- 比较指令CMP
 - 功能: 将目的操作数减去源操作数
 - 按照定义相应设置状态标志
 - 说明: 执行的功能与SUB指令类似, 但结果不回送目的操作数
 - 语法: CMP reg , imm/reg/mem reg—imm/reg/mem

位操作类指令

- 位操作类指令
 - 概述: 以二进制为基本单位进行数据的操作。一类常用的指令
 - 包含
 - 逻辑运算指令
 - ADD(与)
 - 功能: 对两个操作数执行逻辑与运算, 结果送到目的操作数。
 - 语法: ADD des , src des<-des^src
 - OR(或)
 - 功能: 对两个操作数执行逻辑或运算, 结果送到目的操作数
 - 语法: OR dest , src dest<-destv src
 - XOR(异或)
 - 功能: 对两个操作数执行逻辑异或运算, 结果送到目的操作数
 - 语法: XOR dest , src
 - NOT(非)
 - 功能: 对一个操作数执行逻辑非运算
 - 按位取反, 原来的0的位变1, 原来的1的位变0
 - 语法: NOT reg/mem
 - TEST(测试)
 - 移位指令
 - SHL(逻辑左移)
 - SHR(逻辑右移)
 - SAL(算术左移)
 - SAR(算术右移)

- 循环移位指令
 - ROL(左循环移位)
 - ROR(右循环移位)
 - RCL(带进位左循环移位)
 - RCR(带进位右循环移位)

串操作类指令

- 串操作类指令

控制转移类指令

- 控制转移类指令
 - 概述：用于实现分支，循环，过程等程序结构，是仅次于传送指令的常用指令
 - 建议：
 - 重点掌握：JMP/JCC/LOOP、CALL/RET、INT n/IRET 常用系统功能调用
 - 一般了解：LOOPZ/LOOPNZ INTO
 - 包含
 - 无条件转移指令JMP
 - 语法：JMP label
 - 作用：
 - 程序转向label标号指定的地址（标号要在程序其他位置标出）
 - 说明：
 - 只要执行无条件转移指令JMP，不需要任何条件，就使程序转到指定的目的地址处，从目标地址
 - 操作数是要转移到的目标地址开始执行指令
 - 原理
 - 程序的执行地址，是由段寄存器CS和指令指针IP共同确定的，即当前指令的地址为CS：IP
 - 程序的跳转是通过修改CS和IP的值来实现的
 - 条件转移指令JCC
 - 语法：Jcc label
 - 条件满足，发生转移：IP<-IP+8位位移量
 - 条件不满足，顺序执行
 - 说明：
 - 指定的条件cc如果成立，程序转移到由标号label指定的目标地址去执行指令，条件不成立，则程序将顺序执行下一条指令
 - 操作数label是短转移指令，要跳转的地址必须距当前IP地址-128~+127个单元的范围之内
 - Jcc指令不影响标志
 - 但要利用标志
 - 根据利用的标志位不同，16条指令分为3种情况
 - 判断单个标志位状态
 - 比较无符号数高低
 - 比较有符号数大小

- 循环指令LOOP
 - 语法: LOOP label
 - 功能: 循环指令是一种特殊的转移指令, 当满足某条件时, 反复执行一系列操作, 知道不满足为止
 - 说明: 循环指令利用CX寄存器作为计数器
- 子程序指令
 - 语法:
 - 4种类型
 - CALL label; 段内调用, 相对寻址。
 - CALL r16/m16; 段内调用, 间接寻址
 - CALL far ptr label; 段间调用, 直接寻址
 - CALL far ptr mem; 段间调用, 间接寻址
 - 原理:
 - 子程序是完成特定功能的一段程序
 - 当主程序(调用程序)需要执行这个功能时, 采用CALL调用指令转移到子程序的起始处执行
 - 当运行完子程序功能后, 采用RET返回指令回到主程序继续执行
 - 说明:
 - 子程序通常是与主程序分开完成特定功能的一段程序, 程序中有时要反复的实现相同的功能只不过参数不同而已, 把仅参数不同功能重复的程序编写成为子程序, 执行这个功能时, 就可以调用该子程序, 执行完成后在返回主程序。
- 中断指令
 - 语法=中断指令: INT
 - 举例:
 - INT i8
 - 特殊:
 - IRET: 中断返回指令, 实现中断返回
 - INTO: 溢出中断指令
 - 作用: 中断是一种改变程序执行顺序的方法, 在程序运行时, 遇到某些需要紧急处理的情况, 如停电, 数据的实时接收, 溢出等, 处理器暂停主程序的执行, 转去执行中断处理程序。
 - 分类:
 - 内部中断
 - 外部中断

处理器控制类指令

- 处理器控制类指令
 - 概述: 对CPU状态进行控制的指令
 - 包含
 - 空操作指令NOP
 - 语法:
 - NOP CS: SS: DS: ES
 - 作用: 不执行任何操作, 但占用一个字节存储单元, 空耗一个指令执行周期。
 - 用途:
 - NOP常用于程序调试

- 在需要预留指令空间时用NOP填充
- 代码空间多余时也可以用NOP填充
- 还可以用NOP实现软件延时
- 其他
 - LOCK HLT ESC WAIT
- 说明
 - 事实上, NOP和XCHG, AX, 的指令代码一样都是90H
 - 段超越前缀指令: 在允许段超越的存储器操作数之前, 使用段超越前缀指令, 将采用指定的段寄存器寻址操作数
 - CS: 使用代码段的数据
 - SS: 使用堆栈段的数据
 - DS: 使用数据段的数据
 - ES: 使用附加段的数据

伪指令

- 伪指令
 - 概述:
 - 没有对应的机器码的指令, 最终不被CPU所执行
 - 伪指令是由编译器来执行的指令
 - 编译器根据伪指令来进行相关的编译工作
 - 语法:
 - segment和ends是一对成对使用的伪指令
 - 这是在写可被编译器编译的汇编程序时, 必须要用到的一对伪指令
 - segment和ends的功能是定义一个段
 - segment说明一个段开始
 - 语法: 段名 segment
 - ends说明一个段结束
 - 语法: 段名 ends
 - 说明:
 - 一个汇编程序是由多个段组成的, 这些段被用来存放代码, 数据或当作栈空间来使用
 - 一个有意义的汇编程序中至少要有一个段, 这个段用来存放代码
 - 注意:
 - 不要搞混end和ends
 - end是汇编语言的结束
 - 一个汇编程序的结束标记, 编译器在编译汇编程序的过程中, 如果碰到了伪指令end, 就结束对源程序的编译
 - ends是伪指令的结束

ARM汇编语言

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-03 23:06:19

体系架构

- PC端
 - X86
- 移动端
 - ARM

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-03 22:52:19

寄存器

- 寄存器
 - 是什么：存储信息的单元或者说是器件
 - 注：这里讨论的寄存器都是CPU中的寄存器，位于CPU内部，而内存位于CPU外部
 - 使用
 - 对于一个汇编程序员来说，CPU中主要可以使用的也就是寄存器而已
 - 对比
 - 电脑 的内存
 - CPU的寄存器
 - 编程序员可以使用指令来读写CPU中的寄存器，从而实现对于CPU的控制
 - 特点
 - 不同的CPU，寄存器的个数和结构都是不一样的

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新： 2020-08-03 22:51:39

X86寄存器

- 8086 CPU中寄存器总共为14个：且均为16位（32位和64位均以16位为基础）
 - 14个寄存器：AX BX CX DX SP BP SI DI IP FLAG CS DS SS ES
 - 根据类型分
 - 通用寄存器
 - 数据寄存器：AX, BX, CX, DX
 - AX：累加寄存器，也称为累加器
 - BX：基地址寄存器
 - CX：计数器寄存器
 - DX：数据寄存器
 - 指针寄存器：SP和BP
 - SP：堆栈指针寄存器
 - BP：基指针寄存器
 - 变址寄存器：SI和DI
 - SI：源变址寄存器
 - DI：目的变址寄存器
 - 控制寄存器
 - IP：指令指针寄存器
 - FLAG：标志寄存器
 - 段寄存器
 - CS：代码段寄存器
 - DS：数据段寄存器
 - SS：堆栈段寄存器
 - ES：附加段寄存器

x86-64 的调用约定

x86-64 有16个64位寄存器，分别是：

rax, rbx, rcx, rdx, esi, edi, rbp, rsp, r8, r9, r10, r11, r12, r13, r14, r15

寄存器	描述
rax	作为函数返回值使用
rsp	栈指针寄存器，指向栈顶
rdi, rsi, rdx, rcx, r8, r9	依次用作函数参数；如果断点在 OC 方法的第一行，那 rdi 就是 self, rsi 就是 cmd
rbx, rbp, r10, r11, r12, r13, r14, r15	通用寄存器

ARM 寄存器

- ARM寄存器和架构
 - 32位 arm
 - 64位 arm

32位arm的调用约定

寄存器	描述
r0-r3	传递参数与返回值。如果断点在 OC 方法的第一行，那 r0 就是 self, r1 就是 cmd。如果超过四个参数，或者一些例如结构体的参数超过了32位 bit，那么参数将会通过栈来传递；返回值一般都在 r0 上
r4-r6, r8, r10- r11	没有特殊规定，通用寄存器
r7	栈帧指针寄存器(Frame Pointer)，指向下一个保存的栈帧(stack frame)和链接寄存器(link register, lr)在栈上的地址
r9	操作系统保留
r12	IP 寄存器(intra-procedure scratch)
r13	SP 寄存器(stack pointer)，是栈顶指针
r14	LR 寄存器(link register)，存放函数返回后需要继续执行的指令地址
r15	PC 寄存器(program counter)，指向当前指令地址
CPSR	当前程序状态寄存器(Current Program State Register)，在用户状态下存放像 condition 标志中断禁用等标志

arm64的调用约定

arm64有 r0 - r30 是31个通用整形寄存器，PC 不能再作为寄存器直接访问。每个寄存器可以存取一个64位大小的数。当使用 x0 - x30 访问时，它就是一个64位的数。当使用 w0 - w30 访问时，访问的是这些寄存器的低32位。

寄存器	描述
x0–x7	传递参数与返回值。如果参数个数超过了8个，多余的参数会存在栈上；返回值一般都在 x0 上
x29	栈帧指针寄存器(Frame Pointer)，指向一个保存的栈帧(stack frame)和链接寄存器(link register, lr)在栈上的地址
x31	SP 寄存器(stack pointer)，是栈顶指针；根据不同指令，也有可能是 zero register
x30	LR 寄存器(link register)，存放函数的返回地址
CPSR	当前程序状态寄存器(Current Program State Register)，在用户状态下存放像 condition 标志中断禁用等标志

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-08-03 23:06:25

堆栈

- 堆栈
 - 是什么：堆栈都是一种数据项按序排序的数据结构
 - 特点：只能在一端（称为栈顶）对数据项进行插入和删除
 - 堆：队列优先，先进先出
 - 栈：先进后出
 - 功能：暂时存放数据和地址
 - 用途：通常用来保护断电和现场
 - 操作：堆栈中定义了一些操作
 - 两个最重要的是PUSH和POP
 - PUSH操作：在堆栈的顶部加入一个元素
 - POP操作：相反，在堆栈顶部移去一个元素，并将堆栈的大小减一

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-08-03 22:52:40

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

常见术语和名词

- 常见术语和名词
 - 后渗透
 - 红方 蓝方
 - 威胁建模分析
 - PIA分析
 - malware
 - 恶意程序=恶意软件
 - 逆向工程师

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。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-08-02 20:43:11

Web安全

此处整理和Web网络相关的安全相关知识。

- Web安全
 - 根据攻防角度分
 - 进攻
 - 名字和概念
 - 漏洞扫描
 - 端口扫描
 - Web攻击 = Web漏洞攻击
 - Web挖掘 = Web漏洞挖掘
 - Web渗透
 - 攻击方式
 - SQL注入
 - 跨站 XSS
 - CSRF
 - 越权
 - 文件包含
 - 文件上传
 - 命令执行
 - WAF绕过
 - URL跳转
 - 钓鱼
 - 社工 = 社会工程学
 - 防守
 - 代码审计 = 安全代码审计 = 安全审计
 - 目的：写出高质量的漏洞少的代码
 - 日志分析 = 日志关联分析
 - 深度包检测
 - 程序行为监视
 - 防护设备
 - 防火墙
 - WAF = Web应用程序防火墙
 - IDS = Intrusion Detection Systems = 入侵检测系统
 - IPS = Intrusion Prevention Systems = 入侵防御系统
 - 相关组织和标准
 - 组织：OWASP
 - 标准：OWASP10
 - 常见方向和工具
 - 漏洞扫描类
 - AppScan : IBM的一款安全扫描软件
 - AWVS : 一款知名的网络漏洞扫描工具
 - Burp Suite : 一款信息安全从业人员必备的集成型的Web渗透测试工具，价格昂贵的收费软件
 - Cobalt Strike : 一款基于java的渗透测试神器，常被业界称为CS神器

- `Nessus` : 目前全世界最多人使用的Web漏洞扫描与分析软件
- `NetSparker` : 一款综合型的web应用安全漏洞扫描工具
- `Nikto` : 一个开源的Web服务器扫描器, 漏洞扫描神器
- `WebScarab` : 一个用来分析使用HTTP和HTTPS协议的应用程序框架
- `Whisker` : 一款非常好的HTTP服务器缺陷扫描软件, 基于libwhisker
- `ZAP` : OWASP的集成渗透测试和漏洞工具, 免费开源跨平台
- 端口扫描
 - `nmap` : 网络端口扫描嗅探工具
- SQL注入
 - `Sqlmap` : 数据库注入神器
- 主要工作方向和内容
 - 渗透测试
 - 漏洞挖掘
 - 安全开发
 - 代码审计
 - 网络安保

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-02 20:31:07

术语解释

模糊测试

- 模糊测试
 - = fuzz = fuzz testing = fuzzing

渗透测试

- 渗透测试
 - 含义
 - 模拟一种网络攻击，在真正的黑客入侵之前，模拟黑客入侵企业网络来发现薄弱之处
 - 实现方式和常用工具
 - 扫描
 - 端口扫描
 - nmap
 - 漏洞扫描
 - Metasploit
 - 模糊测试
 - Peach = Peach Fuzzer
 - Sulley
 - AutoDafe

漏洞扫描

- 漏洞扫描 = Web漏洞扫描 = Vulnerability Scanning

代码审计

- 代码审计
 - = 代码安全审计 = 安全编码审计 = 源代码审计 = 源代码安全分析
 - 常见工具
 -

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-01 12:40:18

常用工具

此处整理Web安全中常用的一些工具。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-02 20:24:53

安全操作系统

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-02 20:24:38

Kali Linux

- Kali
 - = Kali Linux
 - 旧称: BackTrack Linux
 - 是什么: 一个Linux操作系统, 专门用于渗透测试, 自带大量工具
 - 被称为
 - 网络安全人员的专用系统
 -

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-02 20:26:30

漏洞扫描类

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-01 09:47:13

AppScan

- AppScan
 - = IBM AppScan
 - 一句话介绍：IBM公司开发的用于扫描web应用的基础架构，也是安全渗透行业扛把子的产品

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-08-01 12:18:33

AWVS

- AWVS
 - = Acunetix Web Vulnerability Scanner
 - 一句话描述：一款知名的全能的Web安全漏洞扫描器，并附带有很多实用的工具
 - 通过网络爬虫测试你的网站安全，检测流行安全漏洞

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-08-01 12:20:50

Burp Suite

- Burp Suite
 - 简介
 - 一款信息安全从业人员必备的集成型的渗透测试工具，它采用自动测试和半自动测试的方式
 - 一款专业人员常用的昂贵的工具
 - 特点
 - 收费
 - 有免费的社区版
 - 但功能有限
 - 功能全面
 - 用途
 - 个人常用于暴破，抓包，CSRF测试等等

crifan.com，使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-08-01 12:12:47

Cobalt Strike

- Cobalt Strike
 - = CobaltStrike
 - 一款基于java的渗透测试神器，常被业界人称为CS神器

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-02 20:07:30

Layer

- Layer
 - 简介：一款域名查询工具，可提供网站子域名查询服务
 - 子域名/IP段收集
 - 被称为：Layer子域名挖掘机
 - 作用和特点：
 - 拥有简洁的界面、简单的操作模式
 - 支持服务接口、暴力搜索、同服挖掘三种模式
 - 支持打开网站、复制域名、复制IP、复制CDN、导出域名、导出IP、导出域名+IP、导出域名+IP+WEB服务器以及导出存活网站！
 - 可过滤过出存活主机
- GitHub
 - euphrat1ca/LayerDomainFinder: Layer子域名挖掘机
 - <https://github.com/euphrat1ca/LayerDomainFinder>

TODO:

待整理

子域名搜集思路与技巧梳理 - SecPulse.COM | 安全脉搏

<https://www.secpulse.com/archives/53182.html>

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-08-03 22:26:14

Nessus

- Nessus
 - 一句话介绍：Nessus 是目前全世界最多人使用的Web漏洞扫描与分析软件
 - 总共有超过75,000个机构使用Nessus 作为扫描该机构电脑系统的软件
 - 竞品
 - Burp Suite

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-08-01 12:15:52

NetSparker

- NetSparker
 - 一款综合型的web应用安全漏洞扫描工具
 - 对SQL注入， XSS， LFI等漏洞扫描效果不错的漏洞扫描器

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-08-02 20:06:33

Nikto

- Nikto
 - 一款开源的（GPL）网页服务器扫描器，它可以对网页服务器进行全面的多种扫描

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-08-02 20:03:01

N-Stalker

- N-Stalker
 - 旧称: N-Stealth
 - 是什么: 一款商业级的Web服务器安全扫描程序

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-02 20:05:08

Whisker

- Whisker
 - Whisker是一款基于libwhisker的扫描器，但是现在大家都趋向于使用Nikto，它也是基于libwhisker的

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2020-08-02 20:01:54

Sn1per

- Sn1per
 - 擅长枚举以及扫描已知漏洞
 - 建议这个工具与Metasploit或Nessus一起使用

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-02 20:05:42

WebScarab

- WebScarab
 - 一个用来分析使用HTTP和HTTPS协议的应用程序框架
 - WebScarab记录它检测到的会话内容，使用者可以通过多种形式来查看记录

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-02 20:08:45

Webinspect

- Webinspect
 - = HP Webinspect
 - 惠普公司的安全渗透产品，运行起来占用大量内存，小家碧玉的就慎用了

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-02 20:15:29

Wikto

- Wikto
 - Wikto是一款基于C#编写的Web漏洞扫描工具

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-02 20:03:41

ZAP

- ZAP
 - 名称
 - ZAP = Zed Attack Proxy
 - ZAP = OWASP ZAP
 - 简介
 - 一款开源的Web安全扫描软件
 - 原理
 - ZAP置于浏览器和测试网站之间（又名中间人），允许拦截流量进行检查和修改
 - 竞品
 - Arachni、Wfuzz、Nikto

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-01 12:13:54

端口扫描类

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-01 12:23:44

nmap

TODO:

- 【记录】尝试用nmap去扫描局域网内的计算机的ip和其他详细信息 – 在路上
- nmap
 - =网络扫描仪
 - GUI 版本: Zenmap
 - 包了一个可视化的皮
 - 功能: 扫描端口
 - 就像: 敲门看看你家是否有人
 - 扫描看你开了哪些端口
 - 猜测端口用于何种用途
 - 介绍
 - 不少黑客爱用的工具, 黑客会利用nmap来搜集目标电脑的网络设定, 从而计划攻击的方法
 - 竞品
 - masscan

* 扫全球的时候用

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-03 22:48:53

渗透测试类

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-01 10:06:56

Metasploit

- Metasploit
 - =Metasploit框架=Metasploit项目
 - 简介
 - 世界上使用最广泛的渗透测试框架
 - Metasploit项目是一个旨在提供安全漏洞信息计算机安全项目，可以协助安全工程师进行渗透测试及入侵检测系统签名开发。 Metasploit项目最为知名的子项目是开源的Metasploit框架，一套针对远程主机进行开发和执行"exploit代码"的工具
 - 使用
 - 像是一把弓箭
 - 瞄准目标，选择漏洞，选择有效载荷，然后发射

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-01 10:10:15

模糊测试类

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-01 10:07:21

代码审计类

- 工具
 - Checkmarx
 - =Checkmarx CxEnterprise
 - Armorize CodeSecure
 - Fortify
 - =Fortify SCA
 - RIPS

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-01 12:30:42

注入类

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-02 20:18:59

Sqlmap

- Sqlmap
 - 数据库注入神器
 - 自动执行检测、利用SQL注入漏洞并接管数据库服务器的过程
 - 支持
 - MySQL、Oracle、PostgreSQL、Microsoft SQL Server、Microsoft Access、IBM DB2、SQLite、Firebird、Sybase、SAP MaxDB、Informix、HSQLDB和H2

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-02 20:19:23

组织和标准

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-01 09:30:53

OWASP10

- 组织: OWASP
 - 标准: OWASP10 = OWASP Top 10

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-01 09:31:58

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 、 dll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

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-07-31 23:28:32

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](#)

crifan.com，使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-08-02 19:57:29

Windows安全

- CAIN
 - 是什么：Oxid.it开发的一个针对Microsoft操作系统的免费口令恢复和网络嗅探测试工具
 - 特点：在口令破解上很有一套技术
 - 功能
 - 网络嗅探，网络欺骗，破解加密口令、解码被打乱的口令、显示口令框、显示缓存口令和分析路由协议，甚至还可以监听内网中他人使用VOIP拨打电话等。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-08-02 19:40:11

软件逆向

- 软件逆向
 - =软件逆向工程
 - 定义
 - 通过反汇编和调试等手段，分析计算机程序的二进制可执行代码从而获得程序的算法细节和实现原理的技术。
 - 研究对象
 - 没有公开源代码的计算机程序
 - 主要是已经经过编译的二进制可执行代码
 - 举例
 - win32平台上
 - PE文件
 - 常见文件格式
 - exe
 - dll
 - 分类
 - 系统级逆向
 - 大范围分析观察，整体把握
 - 代码级逆向
 - 程序二进制码中提取设计理念和算法
 - 步骤
 - 研究保护方法，去除保护功能
 - 解码/反汇编（目标二进制代码）
 - 反汇编目标软件，定位功能函数
 - 中间语言翻译（汇编或类汇编代码）
 - 分析汇编代码
 - 数据流分析（各级中间语言）
 - 修改汇编代码或还原高级源代码
 - 其他分析和优化（高级抽象代码）
 - 工具
 - Ollydbg：动态追踪工具，插件较多较多
 - Windbg：用户态和内核态调试工具
 - IDA：交互式反汇编器
 - PEID：著名的查壳工具
 - C32Asm：反汇编程序，可直接修改软件内部代码，有十六进制编辑模式
 - 主要应用
 - 软件破解：破解软件的版权让用户不支付授权费用就可以使用软件的全部功能。
 - 病毒和恶意程序的分析：恶意程序的传播机制和危害并设计出解，分析病毒解决办法。
 - 系统漏洞分析：分析漏洞原理，设计补丁程序或者编写利用程序（Exploit）
 - 分析不公开的文件格式，协议等
 - 分析windows或mac平台上的硬件驱动程序编写linux下的相应驱动

- 挖掘消费电子产品的潜能
- 挖掘操作系统未文档化的API，发现更多内幕
- 计算机犯罪取证

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-08-02 20:40:03

Mac安全

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-02 19:38:50

Linux安全

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-02 19:38:57

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

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-07-31 23:07:32

物联网安全

- IoT端：物联网安全

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-07-31 23:19:47

特定设备安全

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-01 09:28:57

WiFi安全

- WiFi安全
 - Aircrack-ng
 - Wifiphisher
 -

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-03 22:33:24

Aircrack-ng

- Aircrack-ng
 - 一句话描述：一种802.11 WEP和WPA-PSK密钥破解黑客工具
 - 可以在捕获到足够的数据包时恢复密码
 - 资料
 - 官网
 - <http://www.aircrack-ng.org>

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-08-03 22:32:14

Wifiphisher

- Wifiphisher
 - 一句话描述：Wifiphisher是个伪造恶意接入点的工具，可针对WiFi网络发起自动化网络钓鱼攻击。
 - 于任务范围，Wifiphisher可致凭证获取或实际的感染

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-08-03 22:33:55

信息存储安全

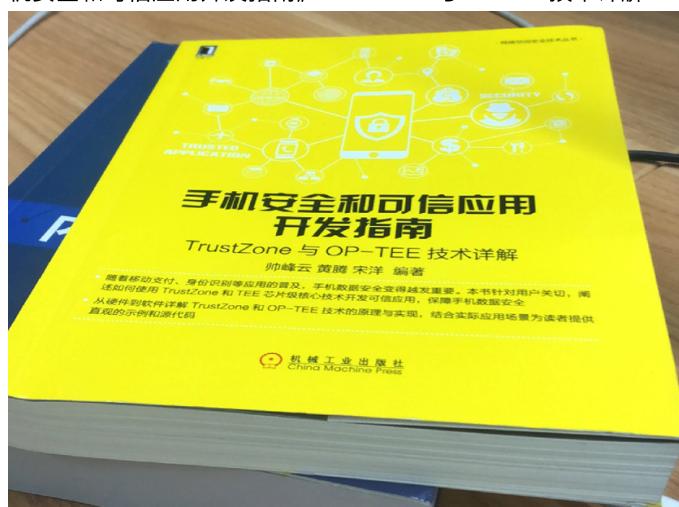
- 信息存储安全

- 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

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

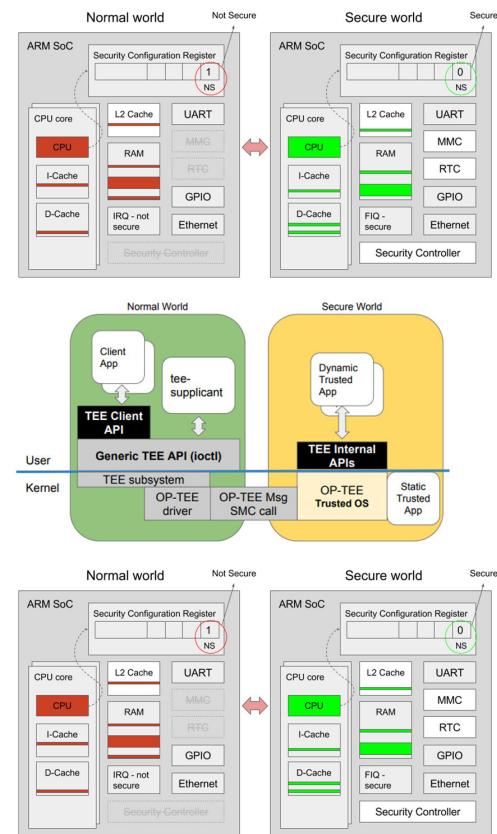
- 对比: Normal world os

- 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`

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-07-31 21:52:19

其他安全相关

安全方面的公司

- Veracode
 - Veracode提供一个基于云的应用程序安全测试平台
 - 无需购买硬件，无需安装软件，使用客户马上就可以开始测试和补救应用程序，另外Veracode提供自动化的静态和动态应用程序安全测试软件和补救服务

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-03 22:28:43

相关技术和工具

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-01 12:27:15

抓包工具

- 网络流量分析 = 网络报文监听 = 网络协议分析
 - Wireshark

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-03 22:28:11

Wireshark

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-03 22:28:24

破解密码

- John the Ripper
- Hashcat
- Hydra

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-03 22:37:42

John the Ripper

- John the Ripper
 - 用GPU算力离线破解密码

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-03 22:30:03

Hashcat

- Hashcat
 - 评价
 - 世界上最快、最先进的密码恢复实用程序
 - 破解哈希的首选渗透测试工具
 - 功能
 - 支持多种猜测密码的蛮力攻击
 - 包括字典和掩码攻击
 - 说明
 - Hashcat在现代GPU显卡上运行最好
 - 传统的hashcat仍支持CPU上的哈希破解
 - 但是要提醒用户的是，这比显卡的处理能力要慢得多

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-03 22:37:17

Hydra

- Hydra
 - 可用于在线破解密码
 - 举例：SSH或FTP登录、IMAP、IRC、RDP等

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-08-03 22:37:45

代理工具

- 常见代理工具
 - Fiddler
 - 常用的抓包工具，有XSS自动化扫描插件
 - parosproxy
 - 一个对Web应用程序的漏洞进行评估的代理程序

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-02 19:41:03

附录

下面列出相关参考资料。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-03-17 09:11:34

资料和文档

安全领域相关论坛

- 常见安全相关网站
 - tools
 - 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，网站依然展示升级公告。
 - 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/>

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-07-31 21:36:29

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
- 「网络安全」安全设备篇（防火墙-IDS-IPS） - 知乎
- 使用peach进行模糊测试从入门到放弃 - 安全客, 安全资讯平台
- Cain & Abel v4.9.44发布 - FreeBuf网络安全行业门户
- Layer子域名挖掘机5.0 SAINTSEC更新版 - 安全工具 - 互联网之家
- Layer子域名挖掘机 - guojia000 - 博客园
- 逆向分析之常见的汇编指令 - FreeBuf网络安全行业门户
- 十大黑客常用渗透测试工具 - 知乎
- 渗透测试专业人员使用的11种工具 - FreeBuf网络安全行业门户
-

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-08-03 22:34:59