

مهندسی معکوس نرم افزارهای موبایل

www.ketab.ir

تألیف: سید داود ملک حسینی

(گروه امنیتی هامان)

انتشارات پندار پارس

سرشناسه	: ملک حسینی، سید داود، ۱۳۶۷-
عنوان و نام پدیدآور	: مهندسی معکوس نرم افزارهای موبایل /تالیف سید داود ملک حسینی.
مشخصات نشر	: تهران : پندار پارس، ۱۴۰۰.
مشخصات ظاهری	: ۱۲۲ص.
شابک	: 978-622-7785-00-5
وضعیت فهرست نویسی	: فیبا
موضوع	: تلفن همراه -- برنامه های کامپیوتری
موضوع	: Cell phones -- Computer programs
رده بندی کنگره	: ۶۵۷۰TK
رده بندی دیویی	: ۲۶۸/۰۰۵
شماره کتابشناسی ملی	: ۷۷۲۷۶۶۴
اطلاعات رکورد کتابشناسی	: فیبا

www.ketab.ir



انتشارات پندار،

دفتر فروش: انقلاب

تلفن: ۶۶۵۷۲۳۳۵

نام کتاب	: مهندسی معکوس نرم افزارهای موبایل
ناشر	: انتشارات پندار پارس
تالیف	: سید داود ملک حسینی
چاپ نخست	: تیر ماه ۱۴۰۰
شمارگان	: ۲۰۰ نسخه
طرح جلد	: رامین شکرالهی
چاپ، صحافی	: روز

شابک : ۹۷۸-۶۲۲-۷۷۸۵-۰۰-۵

: ۷۵۰۰۰ تومان

قیمت

* هرگونه کپی برداری، تکثیر و چاپ کاغذی یا الکترونیکی از این کتاب بدون اجازه ناشر تخلف بوده و پیگرد قانونی دارد *

فصل ۱: معکوس سازی سیستم های DRM در اندروید ۳

۱ مقدمه ۳

۱.۱ Slide Lock چیست و چرا از اهمیت ویژه ای برخوردار است؟ ۵

۱.۲ پیدا کردن کلاس های Slide Lock ۶

۱.۳ آنالیز کردن کلاس ها ۶

۱.۴ پیدا کردن کلاس مربوط به تولید کنندگان ۱۰

۱.۵ وصله کردن / حذف کردن DRM ۱۲

۱.۶ وصله کردن عبارت Switch ۱۲

۱.۷ تغییر دادن کلاس Start up ۱۳

۱.۸ کلید نرم افزار ۱۴

۱.۹ نتیجه گیری ۱۴

فصل دوم: جلیبریک آیفون و آی پد ۱۵

۲. موارد اصلی و پایه ای ۱۶

۲.۱ ابزارها ۱۶

۲.۱.۱ JAILBROKEN IPHONE یا آی پد تاج ۱۶

۲.۱.۲ آید ۵.۲ یا نسخه جدیدتر ۱۶

۲.۱.۳ هگز ادیتور ۱۶

۲.۱.۴ کلانیت SFTP/SSH ۱۷

۲.۱.۵ ابزارهای مورد نیاز روی iDEVICE ۱۷

۲.۲ ساختار فایل نرم افزارها ۱۸

۲.۳ ARM OPCODE ۱۸

۲۰	۲.۴	پروسه پاک کردن APPLE'S DRM
۲۱	۲.۵	ایجاد تغییرات در نرم‌افزار در هنگام عملیات کرک شدن
۲۱	۲.۵.۱	تغییرات روی فایل INFO.PLIST
۲۲	۲.۵.۲	پاک کردن فایل ITUNESMETADATA.PLIST
۲۳	۲.۵.۳	وجود فولدر CODESIGNATURE و CODERESOURCES
۲۳	۲.۵.۴	CRYPTID: LC_ENCRPTION_INFO
۲۴	۲.۶	نمونه‌ها
۲۴	۲.۶.۱	FULL SCREEN WEB BRPWSER
۲۸	۲.۶.۲	RoBO 1.1.2
۳۰	۲.۶.۳	FACES VISUAL DIALER 1.2.1
۳۱	۲.۶.۴	MBOX MAIL 2.01
۳۴	۲.۶.۵	EXZEUS 1.3
۳۹	۲.۶.۶	CONVERTBOT 1.1
۴۱	۲.۶.۷	ZEN BOUND 1.2.1
۴۲	۲.۷	نتیجه گیری
۴۵		فصل سوم: مهندسی معکوس سیستم جیلبریک آیفون
۴۶	۳	جیلبریک کردن IPHONE
۴۸	۳.۱	پروسه جیلبریک کردن سریع و عملی
۵۰	۳.۱.۱	استفاده از IPLUS جهت آی پد کردن
۵۲	۳.۱.۲	استفاده از ZIPHONE برای آی پد کردن
۵۵	۳.۲	ساختار فایل سیستمی
۵۶	۳.۳	دیس اسمبل کردن نرم‌افزارهای ابتدایی از پیش نصب شده
۵۷	۳.۴	نکات مهم موجود در فایل فرست MACH-O
۶۴	۳.۵	نکات مهم روی مدل برنامه‌نویسی شی‌گرای C

۳.۶ نکات مهم روی عملیات معکوس کردن زبان شی‌گرای C: نقش مؤثر	۶۶
OBJC_MSGSEND	۶۶
پارامترها	۶۷
مقدار بازگشتی	۶۷
توضیحات	۶۷
نکات مهم	۶۸
۳.۷ با نگاهی عمیق‌تر بررسی می‌کنیم	۶۸
۳.۸ اولین نرم‌افزارمان را معکوس می‌کنیم	۷۰
۳.۹ اشیاء CFSTRINGS و رشته‌های معمولی و عادی	۷۰
۳.۱۰ انتخاب کننده‌ها-نگه دارنده‌های نقشه	۷۲
۳.۱۱ شکستن قفل آی پد تاج / آیفون	۷۴
۳.۱۲ SCREENSHOTS	۷۷
۳.۱۳ اتصال کامپیوتر به دستگاه	۷۷
۳.۱۴ معکوس کردن برخی نرم‌افزارها	۸۰
۳.۱۴.۱ ACCELEROLOG، اولین نرم‌افزار مورد بررسی	۸۰
۳.۱۴.۲ وصله کردن نرم‌افزار	۸۷
۳.۱۴.۳ چگونه محاسبه Opcode از یک شاخه در ASM	۸۸
۳.۱۵ بررسی دومین نرم‌افزار: SHOWTIME	۹۲
۳.۱۵.۱ نسخه 1.1B	۹۳
۳.۱۶ بررسی سومین نرم‌افزار: ISIM	۹۷
۳.۱۶.۱ از طریق فایل PLIST	۹۸
۳.۱۶.۲ معکوس کردن نرم‌افزار آزمایشی	۹۸
۳.۱۶.۳ تغییر دادن کلاس یک بخش از داده به کد	۱۰۱
۳.۱۶.۴ وصله کردن نرم‌افزار	۱۰۳

سید داود ملکی حسینی

باصیرام

www.ketab.ir

مقدمه
در این کتاب به بررسی و تحلیل آثار و تفکرات سید داود ملکی حسینی پرداخته شده است. این کتاب به گونه‌ای تدوین شده که به منظور آشنایی بیشتر با اندیشه‌های این بزرگوار و همچنین به منظور ارائه تصویری جامع از شخصیت و آثار او به خوانندگان عزیز گردیده است. در این کتاب به بررسی آثار و تفکرات سید داود ملکی حسینی در زمینه‌های مختلف از جمله فلسفه، ادبیات، تاریخ و فقه پرداخته شده است. این کتاب به گونه‌ای تدوین شده که به منظور آشنایی بیشتر با اندیشه‌های این بزرگوار و همچنین به منظور ارائه تصویری جامع از شخصیت و آثار او به خوانندگان عزیز گردیده است.

در این کتاب به بررسی و تحلیل آثار و تفکرات سید داود ملکی حسینی پرداخته شده است. این کتاب به گونه‌ای تدوین شده که به منظور آشنایی بیشتر با اندیشه‌های این بزرگوار و همچنین به منظور ارائه تصویری جامع از شخصیت و آثار او به خوانندگان عزیز گردیده است. در این کتاب به بررسی آثار و تفکرات سید داود ملکی حسینی در زمینه‌های مختلف از جمله فلسفه، ادبیات، تاریخ و فقه پرداخته شده است. این کتاب به گونه‌ای تدوین شده که به منظور آشنایی بیشتر با اندیشه‌های این بزرگوار و همچنین به منظور ارائه تصویری جامع از شخصیت و آثار او به خوانندگان عزیز گردیده است.

پیش‌گفتار