

مقدمه‌ای بر مهندسی امنیت

۱۴۴۴۱۸۲

مؤلفین

دکتر سعید معصومی

(عضو هیئت علمی دانشگاه آزاد اسلامی، احمد اسلامشهر عضو کمیته علمی انجمن رمز ایران)

مهندس سید حسن عسینی



**NAGHOOS
PUBLICATION**

۱۴۴۴۱۸۵

سرشناسه	معصومی، مسعود، ۱۳۵۲ -
عنوان و نام پدیدآور	مقدمه ای بر مهندسی امنیت / مولفین: مسعود معصومی، سید حسن حسینی
مشخصات نشر	تهران: انتشارات ناقوس، ۱۳۹۵.
مشخصات ظاهری	۲۳۶ ص.
شابک	۹۷۸-۹۶۴-۳۷۷-۹۱۷-۷ : بها ۲۲۵۰۰۰ ریال
وضعیت فهرست نویسی	فیب
موضوع	حمله های کانال جانبی
موضوع	Side-Channel attacks :
موضوع	کامپیوتر ها - ایمنی اطلاعات
موضوع	Computer security :
موضوع	شبکه های گسترده (شبکه های کامپیوتری) - تدابیر ایمنی
موضوع	Wide area networks (Computer networks) -- Security measures :
شماره افزوده	حسینی، سید حسین، ۱۳۵۱ -
رده بندی کنگ	QAV۶ /۹ : ۱۳۹۵ م ۶۶ /۹
رده بندی دیویی	۰۰۵/۸
شماره کتابخانه ملی	۲۳۰۷۶۱



برای دیدن آدرس به آدرس زیر مراجعه کنید:

www.naghoos-res.com

انتشارات ناقوس

چاپ اول

S.M.S : ۳۰۰۰۴۵۲۳۲۳

نوبت چاپ اول از دستگاه چاپ دیجیتال استفاده شده است

کلیه حقوق برای ناشر محفوظ است.
تکثیر تمامی یا قسمتی از این اثر به صورت حروفچینی یا چاپ مجدد، چاپ افست، پلی کپی، فتوکپی و انواع دیگر چاپ ممنوع است و پیگرد قانونی دارد.

نام کتاب	مقدمه ای بر مهندسی امنیت
ناشر	انتشارات ناقوس
مولفین	دکتر مسعود معصومی، مهندس سید حسن حسینی
چاپ اول	۱۳۹۵ :
تیراژ	۲۰۰ جلد :
چاپ و صحافی	نارنجستان :
سرپرست صفحه آرا	ربابه موسوی خواه :
قیمت	۲۲۵۰۰۰ ریال :
شابک	۹۷۸-۹۶۴-۳۷۷-۹۱۷-۷ :
ISBN	978-964-377-917-7 :

مرکز پخش: انتشارات ناقوس

۱- خیابان انقلاب-خیابان ۱۲ فروردین- بین وحیدنظری و روانمهر- بن بست حقیقت- پلاک ۴

تلفن و فاکس: ۶۶۳۷۸۹۵۸-۶۶۳۷۸۹۵۷

۲- کتابفروشی الیاس: خیابان انقلاب، نبش ۱۲ فروردین تلفن: ۶۶۴۰۵۰۸۴

۳- کتابفروشی گلریزان: ضلع جنوب شرقی میدان انقلاب، پلاک ۱۱ تلفن: ۶۶۹۷۶۲۳۰

بیوگرافی مولفین

دکتر مسعود معصومی

مسعود معصومی در شهر تهران متولد شد و تحصیلات ابتدایی تا متوسطه را در آنجا به اتمام رساند. وی در سال ۱۳۷۴ در مقطع کارشناسی رشته مهندسی برق گرایش الکترونیک دانشگاه گیلان با عنوان دانشجوی رتبه اول فارغ التحصیل گردید. مسعود معصومی در سال ۱۳۷۹ در مقطع کارشناسی ارشد رشته مهندسی الکترونیک از دانشگاه صنعتی خواجه نصیرالدین طوسی با عنوان دانشجوی رتبه اول و در سال ۱۳۸۵ از همان دانشگاه در مقطع دکترا در رشته الکترونیک با گرایش پیاده سازی سیستم های پردازش سیگنال، کدینگ و رمزنگاری بصورت مجتمع فارغ التحصیل شد. وی در سال ۱۳۸۸ پس از گذراندن یک دوره تحقیقاتی دو ساله در زمینه امنیت سخت افزار و حملات کانال جانبی از دانشگاه صنعتی خواجه نصیرالدین طوسی در مقطع فرا دکترا فارغ التحصیل گردید. ایشان از ۱۳۸۶ تاکنون به عنوان عضو هیات علمی دانشگاه آزاد اسلامی واحد اسلامشهر مشغول به فعالیت های آموزشی و پژوهشی می باشد.

مهندس سیدحسن حسینی

سیدحسن حسینی در شهر تهران متولد شد و تحصیلات ابتدایی تا متوسطه را در آنجا به اتمام رساند. ایشان در سال ۱۳۷۷ در مقطع کارشناسی رشته مهندسی مخابرات و در سال ۱۳۸۷ در مقطع کارشناسی ارشد رشته مهندسی مخابرات گرایش مخابرات های بی سیم فارغ التحصیل شد. وی پس از فارغ التحصیلی مشغول فعالیت های آموزشی و پژوهشی در دانشگاه آزاد اسلامی واحد اسلامشهر بوده و مدتی نیز به عنوان مدرس مدعو دانشگاه آزاد اسلامی واحد اسلامشهر فعالیت داشته اند.

فهرست مطالب

۱۵	فصل اول : انگیزه‌ها و اهداف
۱۵	۱-۱) انگیزه‌ها
۱۹	۲-۱) مدل امنیت
۲۰	۳-۱) حمله سخت افزاری
۲۱	۴-۱) حملات نرم افزاری
۲۲	۵-۱) الزامات امنیتی ماژولهای رمزنگاری
۲۲	۱-۵-۱) اهداف ایتم
۲۲	۲-۵-۱) سطوح ایتمی
۲۴	۳-۵-۱) الزامات ایتمی
۲۴	۴-۵-۱) خط مشی امنیت
۲۵	۶-۱) مهندسی امنیت
۲۵	۷-۱) منابع و مراجع
۲۷	فصل دوم : تهدیدات محتمل در امنیت سخت افزار
۲۹	۱-۲) تهدیدات فیزیکی و مهندسی معکوس تراشه‌ها و سازه‌ها
۳۴	۱-۱-۲) مهندسی معکوس ورود مدار چاپی
۳۶	۲-۲) حملات تهاجمی
۳۸	۱-۲-۲) حملات ریز پروب گذاری
۴۰	۲-۲) حملات غیر تهاجمی و تهدیدات کانال جانبی
۴۱	۱-۳-۲) نشت اطلاعات از تراشه‌های CMOS
۵۲	۲-۲) بسترهای اندازه گیری توان و تشعشعات الکترومغناطیس
۵۲	۱-۴-۲) ابزار تحت حمله
۵۲	۲-۴-۲) اسپلوسکوپ
۵۲	۳-۴-۲) پروب‌های جریان
۵۳	۴-۴-۲) حسگرهای مغناطیسی
۵۴	۵-۴-۲) تقویت کننده کم نویز
۵۴	۶-۴-۲) موتور X-Y-Z
۵۴	۷-۴-۲) رایانه
۵۶	۵-۲) مورد استاندارد ارزیابی حملات کانال جانبی
۵۸	۶-۲) حملات نیمه-تهاجمی
۶۰	۷-۲) منابع و مراجع

۶۲	فصل سوم : حمله القا خطا
۶۳	۱-۳ آسیب پذیری سیستم‌های رمزنگاری در برابر حمله القا خطا
۶۳	۱-۱-۳ انواع خطا
۶۵	۲-۱-۳ روش‌های القا خطا
۷۰	۲-۲ چند نمونه از دستگاههای القا خطا
۷۲	۳-۲ مدل‌های خطا
۷۳	۴-۲ حمله القا خطا به سیستم‌های رمز متقارن
۷۳	۱-۴-۲ حمله القا خطا به الگوریتم DES
۸۱	۲-۴-۲ حمله القا خطا به الگوریتم AES
۸۸	۵-۲ حمله القا خطا به سیستم‌های رمز نامتقارن
۸۸	۱-۵-۲ حمله القا خطا به سیستم رمز RSA
۹۴	۲-۵-۲ حمله القا خطا به سیستم رمزنگاری خم بیضوی
۹۹	۶-۳ حمله القا خطا به سیستم‌های رمز جریانی
۹۹	۱-۶-۳ حمله القا خطا به الگوریتم RC۴
۱۰۱	۷-۲ راهکارهای‌های مقابله با حمله القا خطا
۱۰۱	۱-۷-۲ روش‌های عام مقابله
۱۰۸	۲-۷-۲ روش‌های خاص مقابله
۱۰۹	۸-۳ نتیجه گیری
۱۱۰	۹-۳ منابع و مراجع
۱۱۳	فصل چهارم : حمله تحلیل توان
۱۱۳	۱-۴ منابع مصرف توان در یک مدار دیجیتال
۱۱۵	۲-۴ اندازه‌گیری و تخمین توان در مدارات دیجیتال CMOS
۱۱۶	۳-۴ معیارهای کیفیت سیگنال توان مصرفی
۱۱۶	۴-۴ مشخصات آماری سیگنال مصرف توان
۱۱۷	۱-۴-۴ مشخصات یک نقطه منفرد سیگنال مصرف توان
۱۲۴	۲-۴-۴ نشستی یک نقطه از مصرف توان
۱۲۷	۵-۴ تحلیل توان ساده
۱۲۸	۱-۵-۴ حمله به الگوریتم تولید کلید DES
۱۳۰	۲-۵-۴ تحلیل توان الگوریتم تولید کلید AES
۱۳۱	۳-۵-۴ حملات الگو (قالب)
۱۳۶	۴-۵-۴ حملات تصادم
۱۳۸	۶-۴ تحلیل تفاضلی توان
۱۴۱	۱-۶-۴ حمله به امضا دیجیتال RSA

۱۴۱	۷-۴) نگاهی دوباره به تحلیل همبستگی توان
۱۴۲	۸-۴) تحلیل توان در حوزه فرکانس
۱۴۴	۹-۴) نتیجه گیری
۱۴۵	۱۰-۴) منابع و مراجع
۱۴۷	فصل پنجم: روش‌های مقابله با تحلیل توان
۱۴۸	۱-۵) تشریح عمومی روش‌های مقابله با تحلیل توان
۱۵۰	۲-۵) مقاوم سازی در سطح پروتکل
۱۵۱	۳-۵) مقاوم سازی در سطح الگوریتم
۱۵۱	۱-۲-۵) مقابله با تحلیل توان با روش نقاب گذاری
۱۵۲	۲-۲-۵) نقاب گذاری، پیاده‌سازی‌ها و آسیب‌پذیری‌ها
۱۵۴	۳-۲-۵) مثالی از محافظت از الگوریتم رمزنگاری داده استاندارد
۱۵۷	۴-۲-۵) نقاب گذاری الگوریتم رمز پیشرفته استاندارد
۱۶۰	۵-۲-۵) حملات مرتبه دوم توان
۱۶۲	۴-۵) مقابله با تحلیل توان در سطح سخت‌افزار
۱۶۲	۱-۴-۵) پنهان سازی
۱۶۷	۵-۵) مقایسه میان ASIC, FPGA و پیاده‌سازی نرم‌افزاری
۱۶۸	۶-۵) سایر توصیه‌ها مربوط به مقاومت در برابر حمله تحلیل توان
۱۶۹	۷-۵) توصیه‌های طراحی و پیاده‌سازی تراشه رمز
۱۷۱	۷-۵) نتیجه گیری
۱۷۲	۸-۵) منابع و مراجع
۱۷۵	فصل ششم: حمله تحلیل زمان
۱۷۶	۱-۶) مدل حمله تحلیل زمان
۱۷۶	۲-۶) حمله تحلیل زمان علیه سیستمهای رمز متقارن
۱۷۶	۱-۲-۶) نحوه شکستن سیستم رمزنگاری RSA با حمله تحلیل زمان
۱۷۷	۲-۲-۶) الگوریتم مربع کردن و ضرب، ضرب کننده مونتگمری
۱۷۸	۳-۲-۶) شکستن الگوریتم مونتگمری با حمله تحلیل زمان
۱۷۹	۴-۲-۶) حمله تحلیل زمان به الگوریتم استاندارد امضای دیجیتال
۱۸۰	۳-۶) حمله تحلیل زمان علیه رمزهای متقارن
۱۸۰	۱-۳-۶) پیاده سازی حمله
۱۸۱	۲-۳-۶) فاز اندازه گیری
۱۸۱	۴-۶) روشهای مقابله با حمله تحلیل زمان
۱۸۱	۱-۴-۶) اجرای الگوریتم در زمان ثابت
۱۸۲	۲-۴-۶) افزودن نویز

۱۸۳	۳-۴-۶) استفاده از عملگرهای ریاضی ساده
۱۸۴	۴-۴-۶) تصادفی سازی متغیرها
۱۸۴	۵-۶) نتیجه گیری
۱۸۵	۶-۶) منابع و مراجع
۱۸۷	فصل هفتم : حمله تحلیل تشعشعات الکترومغناطیس
۱۸۸	۱-۷) پیش زمینه های انتشار الکترومغناطیس
۱۸۹	۲-۷) انواع تشعشعات الکترومغناطیس
۱۹۰	۳-۷) انتشار امواج الکترومغناطیس
۱۹۳	۴-۷) ابزارهای اندازه گیری EM
۱۹۳	۱-۴-۷) گیرنده های الکترومغناطیس
۱۹۵	۲-۴-۷) پروب های الکترومغناطیس
۱۹۵	۳-۴-۷) آنتن های میدان
۱۹۶	۴-۴-۷) آنتن های حلقوی
۲۰۱	۵-۷) مثالهایی از نشت EM
۲۰۱	۱-۵-۷) مدولاسیون دامنه
۲۰۶	۶-۷) تعدد کانالهای EM و مقایسه آن با سیل توان
۲۰۹	۷-۷) تحلیل ساده، تفاضلی و همبستگی
۲۱۱	۸-۷) حمله تشعشعات الکترومغناطیس مربع
۲۱۵	۹-۷) راهکارهای مقابله با حمله تشعشعات الکترومغناطیس
۲۱۶	۱۰-۷) نتیجه گیری
۲۱۷	۱۱-۷) منابع و مراجع
۲۱۹	فصل هشتم : توابع کپی ناپذیر فیزیکی برای محافظت از اصالت سخت افزار
۲۲۰	۱-۸) انواع PUF های سیلیکونی
۲۲۲	۱-۱-۸) PUF های مبتنی بر نوسان سازهای حلقوی
۲۲۳	۲-۸) بکارگیری PUF برای مقابله با کپی سازی، مهندسی معکوس و نگهداری کلید
۲۲۳	۱-۲-۸) نگهداری امن کلید
۲۲۴	۲-۲-۸) شناسایی ابزار
۲۲۴	۳-۸) منابع و مراجع
۲۲۵	فصل نهم : بررسی اجمالی امنیت پیاده سازی الگوریتم های رمزنگاری بر روی تراشه
۲۲۶	۱-۹) تهدیدات متوجه FPGA
۲۲۷	۲-۹) آسیب پذیری های FPGA
۲۲۸	۱-۲-۹) سطح تکنولوژی
۲۲۹	۲-۲-۹) سطح منطقی

۲۲۰		۲-۲-۹	سطح معماری
۲۲۰		۴-۲-۹	سطح سیستم
۲۲۱		۲-۹	روش های مقابله
۲۲۱		۱-۲-۹	سطح تکنولوژی
۲۲۲		۲-۳-۹	سطح منطقی
۲۲۲		۲-۳-۹	سطح معماری
۲۲۴		۴-۹	نتیجه گیری
۲۲۵		۵-۹	منابع و مراجع

www.ketab.ir

پس از تقریباً ده سال تحقیق و تدریس در زمینه امنیت و سخت‌افزارهای امنیتی، نیاز به یک کتاب فارسی که دربرگیرنده اهم مطالب در این زمینه باشد کاملاً محسوس و ملموس بنظر می‌رسید. لذا بر آن شدم تا بر مبنای تجارب قبلی کتابی را در این خصوص تالیف کنیم تا به درک بهتر موضوع و پر کردن خلا موجود در این زمینه کمک کرده باشیم. با گسترش روزافزون انواع شبکه‌های مخابراتی و تراکنش‌های الکترونیکی و اینترنتی، حفظ امنیت و محرمانگی اطلاعات از جمله مهمترین ضروریات حرکت به سمت دولت الکترونیک بشمار می‌رود. همزمان با رشد بسیار سریع استفاده از کارت‌های اعتباری و هوشمند و سایر توکن‌ها، امنیتی، انواع حملات پیچیده از سوی نفوذگرها که گاه بصورت شخصی و گاه بصورت کامل سازمان یافته سعی در شکستن محرمانگی اینگونه ابزارها دارند نیز گسترش می‌یابد. این کتاب شرح نسبتاً کامل، مربوط و هیجان انگیز و در عین حال هشدار دهنده‌ای از نحوه استفاده از سیگنال‌های کانال جانبی از جمله مصرف توان، تشعشعات الکترومغناطیسی و یا القا خطا برای کشف رمز و شکستن امنیت سامانه‌ها و امنیتی سخت‌افزاری مانند کارت‌های هوشمند یا توکن‌های امنیتی است. ضمن آنکه شرح مختصری از مسائل و مهم پایه امنیت سخت‌افزار، استانداردهای موجود و امنیت فیزیکی سامانه‌های امنیتی سخت‌افزاری را بر می‌گیرد. معمولاً الگوریتم‌های رمزنگاری بلحاظ آماری و ریاضی آنقدر امن هستند که شکستن آنها با استفاده از توان‌های محاسباتی و پردازشی موجود و به روش‌های متعارف تقریباً غیر ممکن است. این کتاب به تشریح روش‌هایی می‌پردازد که شخص کنجکاو را قادر می‌سازد تا در مدت زمانی بسیار کوتاه تر و با هزینه‌ای بسیار کمتر در مقایسه با روش‌های متعارف، از طریق تحلیل نشت اطلاعات از یک سخت‌افزار در حال پردازش اطلاعات و هدف قرار دادن نقاط ضعف پیاده‌سازی الگوریتم‌های امنیتی موجود در آن، کلید رمز یا سایر اطلاعات حساس آن را کشف کند. علاوه بر موارد مطرح شده روش‌های محافظت از سامانه‌های امنیت سخت‌افزاری در برابر این حملات نیز تشریح شده‌اند. مخاطب اصلی این کتاب محققین و دانشجویان کارشناسی ارشد رشته مهندسی الکترونیک، مخابرات و کامپیوتر علاقمند به حوزه امنیت و نیز دست اندرکاران و شاغلین در صنایعی است که بحوری با این مقوله مهم مرتبط هستند. البته برای درک بهتر مطالب کتاب داشتن پیش زمینه رمزنگاری و امنیت لازم است. در تالیف این کتاب از برخی ایده‌ها و کارهای قبلی مولفین نیز استفاده شده است. امید است این کتاب دریچه‌ای هرچند کوچک را بروی محققین و علاقمندان به این موضوع جذاب باز کند. ضمن آنکه بدون شک مطالب ارائه شده خالی از ایراد و اشکال نیست. امید است همکاران و دانشجویان عزیز نقطه نظرات خود را به مولفین منتقل کنند تا ان‌شاءالله در ویراست‌های بعدی مورد نظر قرار بگیرد.