مقدمه‌ای بر مهندسی امنیت

مولفین

دکتر مسعود معصومی

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

مهندس سید حسن حسینی

NAGHOOS
PUBLICATION

۱۴۴۴۱۸۴

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	:۲۳۶ص.
شابک	: ۷-۹۱۷-۳۷۷-۹۶۴- ۹۷۸ بها :۲۲۵۰۰۰ ریال
وضعیت فهرست نویسی	: فیپا
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
شناسه افزوده	: حسینی، سید حسین، ۱۳۵۱-
رده بندی کنگره	: ۱۳۹۵ ۶۶م ۹ک/ ۹/ QA۷۶
رده بندی دیویی	: ۰۰۵/۸
شمارهٔ کتابشناسی ملی	: ۴۴۰۷۶۰

انتشارات ناقوس

چاپ اول

S.M.S : ۳۰۰۰۴۵۲۳۲۳

« این نوبت چاپ اول از دستگاه چاپ دیجیتال استفاده شده است »

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

مرکز پخش: انتشارات ناقوس

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

تلفن و فاکس : ۶۶۳۷۸۹۵۷-۶۶۳۷۸۹۵۸

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

۳- کتابفروشی گلریزان: ضلع جنوب‌شرقی 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 فارغ‌التحصیل گردید. مسعود معصومی در سال ۱۳۷۹در مقطع کارشناسی‌ارشد 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 پیاده‌سازی سیستم‌های پردازش سیگنال، کدینگ و رمزنگاری بصورت مجتمع فارغ‌التحصیل شد. وی در سال ۱۳۸۸ پس از گذراندن یک دوره تحقیقاتی دو ساله در زمینه امنیت سخت‌افزار و حملات کانال جانبی از دانشگاه صنعتی خواجه نصیرالدین طوسی در مقطع فرا دکترا فارغ‌التحصیل گردید. ایشان از ۱۳۸۶ تاکنون به عنوان عضو هیات علمی دانشگاه آزاد اسلامی واحد اسلامشهر مشغول به فعالیت‌های آموزشی و پژوهشی می‌باشد.

مهندس سیدحسن حسینی

سیدحسن حسینی در شهرستان شاهرود 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 کارشناسی‌ارشد رشته مهندسی مخابرات گرایش رمز فارغ‌التحصیل شد. وی پس از فارغ‌التحصیلی مشغول فعالیت‌های آموزشی و پژوهشی در بخش‌های کشور بوده و مدتی نیز به عنوان مدرس مدعو دانشگاه آزاد اسلامی واحد اسلامشهر فعالیت داشته‌اند.

فهرست مطالب

پیشگفتار

پس از تقریبا 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 شدیم 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 توکن‌های امنیتی، انواع حملات پیچیده از سوی نفوذگرها که گاه بصورت شخصی و گاه بصورت کاملا سازمان یافته سعی در شکستن محرمانگی اینگونه ابزارها دارند نیز گسترش می‌یابد. این کتاب شرح نسبتا کامل، مبسوط 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 سامانه‌های امنیتی سخت‌افزاری مانند کارت‌های هوشمند یا توکن‌های امنیتی است. ضمن آنکه شرح مختصری از حملات و مفاهیم پایه امنیت سخت‌افزار، استانداردهای موجود و امنیت فیزیکی سامانه‌های امنیتی سخت‌افزاری را در بر می‌گیرد. معمولاً الگوریتم‌های رمزنگاری بلحاظ آماری و ریاضی آنقدر امن هستند که شکست آنها با استفاده از توان‌های محاسباتی و پردازشی موجود و به روش‌های متعارف تقریبا 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 بنحوی 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 ان‌شاالله در ویراست‌های بعدی مورد نظر قرار بگیرد.

مسعود معصومی m_masoumi@iiau.ac.ir

سیدحسن حسینی shh@pcaspian.ir