حملات تحلیل توان

آشکارسازی اطلاعات محرمانه‌ی کارت‌های هوشمند

نویسندگان:

Stefan Mangard
Elisabeth Oswald
Thomas Popp

مترجم:

اقلیدس

ویراستاران علمی:

مهندس داوود شنبه‌زاده

دکتر مسعود معصومی

سرشناسه: منگرد، استفان Mangard 'Stefan
عنوان و نام پدیدآور: حملات تحلیل توان= آشکارسازی اطّلاعات محرمانه‌ی کارت‌های هوشمند/ نویسندگان استفان منگارد، الیزابت اسوالد، توماس پاپ؛ مترجم اقلیدس؛ ویراستاران علمی داوود شنبه زاده، مسعود معصومی.
مشخصات نشر: تهران: دانشگاه صنعتی مالک اشتر، ۱۳۹۱. مشخصات ظاهری: ی، ۵۵۲ ص.
وضعیت فهرستنویسی: فیپا
یادداشت: عنوان اصلی: Power analysis attacks: revealing the secrets of smart cards ' c2007
عنوان دیگر: آشکار سازی اطّلاعات محرمانه‌ی کارت‌های هوشمند.
موضوع: کارت‌های هوشمند- اقدامات تامینی
شناسه افزوده: آزوالد، الیزابت
شناسه افزوده: Oswald ' Elisabeth
شناسه افزوده: پوپ، تامس، ۱۹۷۸- م.
شناسه افزوده: Popp ' Thomas
شناسه افزوده: اقلیدس، مترجم
شناسه افزوده: شنبه‌زاده، داوود، ویراستار
شناسه افزوده: دانشگاه صنعتی مالک اشتر
رده بندی کنگره: ۱۳۹۱ ۸م۲ک/TK۷۸۹۵ رده بندی دیویی: ۰۰۵/۸ کتابشناسی ملی: ۳۰۹۱۷۱۸

انتشارات دانشگاه صنعتی مالک اشتر

دانشگاه صنعتی مالک اشتر

مجتمع دانشگاهی برق و الکترونیک

عنوان کتاب: ..... **حملات تحلیل توان، آشکار سازی اطّلاعات محرمانه‌ی کارت‌های هوشمند**
مترجم: ..... **آهنگ اقلیدس**
ناشر: ..... **انتشارات دانشگاه صنعتی مالک اشتر**
طرح روی جلد: ..... **فریناز عسگری**
لیتوگرافی، چاپ و صحافی: ..... **انتشارات دانشگاه صنعتی مالک اشتر**
صفحه‌آرایی رایانه ای: ..... **امین پژوهش جهرمی**
ویراستار ادبی: ..... **امین پژوهش جهرمی**
شمارگان: ..... **۱۰۰۰ جلد**
نوبت چاپ: ..... **اول، زمستان ۹۱**
قیمت: ..... **۲۷۰.۰۰۰ ریال**

شابک: ۹-۴۹-۵۶۶۵ - ۶۰۰ -۹۷۸ ISBN: 978-600-5665-49-9

آدرس: تهران، لویزان، دانشگاه صنعتی مالک اشتر، مرکز فناوری اطلاعات و مدیریت دانش،
مدیریت انتشارات. تلفن: ۲۲۹۳۲۸۹۱

استفان منگارد
موسسه پردازشِ اطّلاعاتِ کاربردی و ارتباطات
دانشگاه صنعتی گِراز
اینفلدگاس a ۱۶
۸۰۱۰ گِراز
اتریش

الیزابت اُسوالد
موسسه پردازشِ اطّلاعاتِ کاربردی و ارتباطات
دانشگاه صنعتی گِراز
اینفلدگاس a ۱۶
۸۰۱۰ گِراز
اتریش

توماس پاپ
موسسه پردازشِ اطّلاعاتِ کاربردی و ارتباطات
دانشگاهِ صنعتی گِراز
اینفلدگاس a ۱۶
۸۰۱۰ گِراز
اتریش

شماره‌ی کنترلِ کتابخانه‌ی مجلس: ۲۰۰۷۹۲۳۵۶۵

حملات تحلیل توان: آشکارسازیِ اطّلاعاتِ محرمانه‌یِ کارت‌های هوشمند

توسط استفان منگارد، الیزابت اُسوالد و توماس پاپ

ISBN-13:9780-387-30857-9
ISBN-10:0-387-30857-1
e-ISBN-13:978-0 387 38162-6
e-ISBN-10:0-387-38162-7

چاپ شده روی کاغذ بدون اسید.

9 8 7 6 5 4 3 2 1

springer. com

سخن مترجم

دلایل اهمیت ترجمه کتابِ حملاتِ تحلیلِ توان

۱- این کتاب، نخستین کتاب کامل در جهان است که در سال ۲۰۰۷ میلادی منتشر شده است که به تحلیل کانال جانبی و توان مصرفی (که از نوین‌ترین روش‌ها و فناوری‌های تحلیلِ رمز می‌باشند) پرداخته و تئوری را در کنار تجربیات عملی به خوبی نشان می‌دهد.

۲- این کتاب، روش‌های پیشگیری در برابر تحلیل‌های رمز کانال جانبی را (که در طراحی رمزکننده‌ها باید رعایت شوند و مرجعِ مناسب برای طراحی سامانه‌های رمز است) را به‌طور مبسوط تشریح می‌کند.

۳- تنوعِ مطالب و موضوعِ نوین آن، امکانِ تعریفِ پایان‌نامه‌هایی را فراهم می‌آورد که این کتاب می‌تواند مفیدترین و کامل‌ترین مرجع در این زمینه باشد.

٤- موضوع تحلیل‌های کانال جانبی سامانه‌های رمز در کشور بسیار تازه بوده و تدریس و کار پژوهشی در این زمینه، نیاز به مراجع علمی مناسب دارد.

۵- با توجه به زمان‌بر بودن تحلیل‌های ریاضی و آماری سامانه‌های رمز نوین در دنیا، توجه عمده صاحب‌نظران رشته رمزنگاری و رمزشکنی به حملات کانال جانبی و به‌ویژه حمله تحلیل توان معطوف گشته که این کتاب شرحی بر این موضوع است.

۶- مبحث اصلی این کتاب، شکستن رمز کارت‌های هوشمند با استفاده از حمله تحلیل توان است. با توجه به استفاده رو به رشد و روزافزون کارت‌های هوشمند، کارت‌های بانکی، کارت‌های سوخت و تجارت الکترونیک، مطالب ارایه شده در این کتاب، می‌تواند به ارتقای امنیت این‌گونه سامانه‌ها کمک شایانی کند.

۷- بخش‌هایی از کتاب، به روش‌های نرم و غیرفعال[1] مقاومت و دفاع در برابر حمله‌های کانال جانبی و توان مصرفی پرداخته که می‌تواند مرجع مناسبی برای پدافند غیرعامل رمزکننده‌ها در برابر این نوع حمله‌ها باشد.

۸- نمونه‌کارهای عملی این کتاب، امکانِ اجرای مثال‌ها و راه‌اندازی آزمایشگاهِ مرجعِ تحلیلِ رمز را می‌دهد.

[1] Passive

پیش‌گفتار

"ما الکتریسیته را درک نمی‌کنیم؛ آن را به‌کار می‌بریم."

-- **مایا آنجلو**

هنگامی که پژوهش‌های خود را در زمینه "مقاومت در برابر نفوذ" آغاز کردم، استطاعت مالی لازم برای خرید تجهیزات مورد نیاز برای تحلیل و مهندسی معکوس حملات فیزیکی را نداشتم. این مساله مشکل بسیار بزرگی ایجاد کرد: مشتریانِ شرکت ، نتایج پژوهش‌های علمی را می‌خواستند، ولی نمی‌توانستم روش‌های حمله‌ای را به کار ببرم که در آن زمان معروف بودند.

با پرسشی ساده آغاز کردم: چه اطلاعاتی در اختیار مهاجمین قرار دارد که در پروتکل‌های رمزنگاری در نظر گرفته نشده است؟

پیش‌تر کشف کرده بودم که تغییرات زمانیِ دقیق، می‌تواند کلیدها را مورد تهدید قرار دهد، بنابراین تصمیم گرفتم دریابم آیا مصرف توان می‌تواند اطلاعات ارزشمندی را افشاء کند. ساعت‌ها پس از حمل دشوار یک اُسیلوسکوپ آنالوگ ۵۰۰ دلاری به خانه (خریداری شده از مغازه‌ی الکترونیکی Fry)، من و همکارِ پژوهشی‌ام **جوشوا جافی**[1] نخستین تریس‌های مصرف توان‌مان را مشاهده کردیم.

با کارت هوشمندی که الگوریتم RSA[2] را اجرا می‌کرد آغاز کردیم، و دریافتیم که می‌توانیم ویژگی‌های عمده‌ی این الگوریتم را شناسایی کنیم. به زودی، آموختیم

---

[1] Joshua Jaffe

[2] Rivest- Shamir- Adleman

می‌توان تفاوت‌های میان مراحل توان‌رسانی و ضرب را تشخیص داد و نخستین کلیدمان را با کاربرد SPA[1] پیدا کردیم. هم‌چنین، پیاده‌سازی‌های DES[2] را تحلیل کردیم؛ و دریافتیم که آن‌ها را نیز می‌توان شکست، گرچه تنها در شب_ نور روز در اداره تصویر اُسیلوسکوپ ارزان قیمت را کم‌رنگ می‌کرد.

طی ماه‌های بعد، سامانه‌های ثبت داده‌های دیجیتال را ساختیم، که تحلیل پیچیده‌تری را ممکن می‌ساخت. هم‌چنین نرم‌افزار دیداری را توسعه دادیم و روش‌های تحلیل بسیاری از جمله تحلیل تفاضلی توان را اجرا کردیم. محصولات بی‌شماری را آزمایش کردیم؛ هر کارت هوشمند و هر ابزار مقاوم در برابر نفوذ دیگری را که آزمایش کردیم قابل شکسته شدن بودند.

توان DPA هم شگفت‌انگیز بود و هم وحشت‌آور.

به طور موازی، انرژی زیادی را صرف توسعه‌ی روش‌های مقابله کردیم.

حل این مشکل نیرنگ‌آمیز است؛ زیرا آمارهای مورد استفاده در حمله تحلیل تفاضلی توان می‌تواند همبستگی‌های ناچیزی که در نویز وجود دارد را شناسایی کند. به‌طور مشابه، حذف نشت اطلاعات کمابیش غیرممکن است؛ زیرا حرکت الکترون‌ها به‌طور یکنواخت الکتریسیته مصرف کرده و میدان‌های الکترومغناطیسی تولید می‌کند.

هم‌اکنون، شرکت من برای امتیازات بیرون آمده از این کار، پروانه صادر می‌کند. اگر در حال ساخت محصولاتی با استفاده روش‌های مقابله حمله DPA هستید، آگاه باشید که این امتیازات وجود دارند، نمی‌خواهم مردم یا شرکت‌ها شگفت‌زده شوند. جالب است که SPA و حمله تحلیل تفاضلی توان برای مدت زمان طولانی کشف نشدند. دلیل اصلی ساده است: هیچ‌کس در پی یافتن موضوع نبود.

رمزنگاران بر دست‌یابی به قدرت ریاضی تمرکز کرده بودند، در حالی که مهندسان پاسخ‌گوی مسائل نرم‌افزار و سخت‌افزار بودند. پژوهش‌های حمله نیز به‌طور مرتب

[1] Simple Power Analysis
[2] Data Encryption Standard

تنها روی الگوریتم‌ها تقسیم‌بندی شده بودند، و از راه‌های دفاعی فیزیکی جدا شده بودند. تعداد کمی از رمزنگاران روی محصولات واقعی کار می‌کردند، و تعداد کمی از مهندسان، ریاضیات می‌دانستند.

امیدوارم در حال خواندن این کتاب به مشکلات امنیتی که به آن‌ها توجه نشده فکر کنید. در سال‌های پس از عمومی شدن حمله تحلیل تفاضلی توان، پژوهش‌های عمیق روی مقاومت در برابر نفوذ، پیشرفت‌های بسیاری داشته‌اند.

همه کنفرانس‌ها روی این موضوع متمرکز شده‌اند. پژوهش‌گرانی مانند مولف این کتاب و دیگران حملات DPA را در جهت‌های جدیدی به‌کار برده‌اند. محصولات امنیتی نیز بسیار بهبود یافته‌اند.

با آن‌که بیش‌تر محصولاتی که به‌وسیله‌ی شرکت من بررسی شده است هم‌چنان دارای آسیب‌پذیری‌هایی نسبت به حمله تحلیل تفاضلی توان است، بهترین محصولات ارایه شده دارای راهکارهایی برای مقابله در برابر این حمله‌ها هستند. فروشندگان نیز دریافته‌اند که مقاومت در برابر نفوذ مساله دشواری است، و ادعاهای امنیتی آن‌ها بسیار دور از واقعیت است. با نگاهی به آینده، مقاومت در برابر نفوذ، هم‌چنان به عنوان علاقه‌مندی بسیار بزرگ و مساله‌ای مهم باقی خواهد ماند.

در سال ۲۰۰۷ بالغ بر ۲ میلیارد تراشه مقاوم در برابر نفوذ برای ارتباطات امن، پرداخت‌ها، موارد مصرفی چاپگر، پرداخت سامانه‌های تلویزیون[1]، IDهای دولتی و کاربردهای بی‌شمار دیگر تولید خواهند شد. حملات علیه نیمه‌رساناهای مقاوم در برابر نفوذ، عامل میلیاردها دلار جعل و سرقت شده است. به‌عنوان یک قانون، پروتکل‌های رمزنگاری فقط به میزان پارامترهای امنیتی درون آن‌ها اهمیت می‌دهند، بی‌شک هم‌چنان موارد بسیار زیادی در رابطه با چگونگی ذخیره‌سازی و مدیریت ایمن کلیدها وجود دارد که ناشناخته مانده‌اند.

[1] TV

شما این کتاب را شگفت‌انگیز، جالب و اخطاردهنده خواهید یافت.

در حین مطالعه آستین‌های خود را بالا بزنید.

پرسش‌های بدبینانه بپرسید.

در کنفرانس‌های پژوهشی شرکت کنید.

از قوانین پیروی کنید و بالاتر از همه موارد بالا، شاد باشید.

پاول کوچر[1]

رئیس و سرپرست شرکت پژوهشی رمزنگاری

سان فرانسیسکو- سپتامبر ۲۰۰۶ میلادی

[1] Paul Kocher

دیباچه

حملاتِ تحلیلِ توان، تحلیل‌های رمزنگاری هستند که اجازه‌ی استخراجِ اطلاعاتِ محرمانه را از ابزارهای رمزنگاری می‌دهند. در برابر دیگر حملات رمزنگاری، آن‌ها مشخصات توان مصرفی ابزارها را به‌جای خواص ریاضی الگوریتم‌های رمزنگاری مورد بهره‌برداری قرار می‌دهند.

حملات تحلیل توان، از نوع غیرتهاجمی هستند که می‌توانند با تجهیزاتی عمومی و قابل دسترس اجرا و پیاده‌سازی شوند. بنابراین، این‌گونه تحلیل‌ها می‌توانند تهدیدی جدی برای امنیت ابزارهای رمزنگاری مانند کارت‌های هوشمند باشند.

کارت‌های هوشمند، عمومی‌ترین نوع ابزارهای رمزنگاری هستند. طبقِ گزارش یوروواسمارت[1]، مجمع بین‌المللی شرکت‌های (سازنده) کارت هوشمند، بازارِ کسب و کار برای این کارت با ریزپردازنده‌ها در مدت چند سالِ اخیر، بیش از دو برابر شده است.

در سال ۲۰۰۳، کم‌تر از یک میلیارد کارت ساخته شده است؛ در حالی که انتظار می‌رود در سال ۲۰۰۶ در حدود دو میلیارد کارت فروخته شوند. بیش‌ترِ این کارت‌ها در کاربردهای حساس امنیتی، مانند ارتباطات از راه دور، سرویس‌های مالی، سرویس‌های دولتی، امنیت سرویس‌های اشتراکی، پرداخت‌های تلویزیون و تلویزیون کابلی به‌کار رفته‌اند.

---

[1] Eurosmart

کارت‌های هوشمند، مولفه حیاتی این کاربردها هستند؛ بنابراین امنیت آن‌ها ضروری است. به‌دلیل نیاز به توسعه اقدامات دفاعی و پیشگیرانه، پژوهش‌گران بررسی در جزئیات حملات تحلیل توان را آغاز کردند. حملات تحلیل توان به زمینه جذابی برای تحقیق تبدیل شده‌اند.

درک آن‌ها به دانستن حوزه‌های فناوری مختلف مانند رمزنگاری، آمار، فناوری اندازه‌گیری، و میکروالکترونیک نیاز دارند که توجه همه پژوهش‌گران این زمینه‌ها را جلب کرده‌اند. در نتیجه، تعداد زیادی از مقالات تحقیقی در طی چند سال اخیر منتشر شده‌اند. در حقیقت، این مساله دنبال کردن تمامی این مستندات و درک این که این ایده‌ها چگونه به یکدیگر مرتبط هستند، تبدیل به مساله‌ای کاملا چالش‌برانگیز شده است.

افزون بر این، هیچ نوشتار مقدماتی برای آشنا کردن علاقه‌مندان با همه‌ی انواع حملات تحلیل توان و اقدامات متقابل برای جلوگیری از آن وجود ندارد.

هدف این کتاب پُر کردن این فضای خالی است. در این کتاب، آشنایی جامعی با حملات تحلیل توان فراهم می‌کنیم.

در آغاز با بحثی در مورد ابزارهای رمزنگاری، طراحی و توان مصرفی آن‌ها، آمار و مهندسی الکترونیک را در کنار یکدیگر آوردیم تا انواع مختلف حملات تحلیل تفاضلی توان و روش‌های مقابله با آن را تشریح و تحلیل کنیم.

این کتاب به همان اندازه که برای پژوهش‌گران نوشته شده، برای افراد شاغل با پیش‌زمینه‌های رمزنگاری، امنیت، یا میکروالکترونیک نیز مفید است.