حمله RAMBO
و نفوذ به سیستم‌های ایزوله از طریق کانال‌های جانبی

مفهوم حملات کانال جانبی

حملات کانال جانبی به روش‌هایی اطلاق می‌شود که در آن مهاجم بدون دسترسی مستقیم به داده‌های رمزنگاری‌شده یا اطلاعات حساس، از منابع جانبی نظیر مصرف توان، صدا، الکترومغناطیس، حرارت یا زمان اجرای عملیات‌ها برای استخراج اطلاعات بهره می‌برد. این حملات برخلاف حملات نرم‌افزاری سنتی، بیشتر مبتنی بر تحلیل سیگنال‌های فیزیکی هستند.

ضرورت بررسی موضوع

در عصر وابستگی شدید به سیستم‌های دیجیتال و استفاده از سامانه‌های ایزوله (air-gap) برای حفاظت از داده‌های حیاتی، کشف و تحلیل حملاتی که حتی این محیط‌های ایمن را تهدید می‌کنند، اهمیت بالایی دارد. حملاتی چون RAMBO ثابت می‌کنند که حتی در نبود اتصال شبکه‌ای، امکان نشت اطلاعات از طریق کانال‌های پیش‌بینی‌نشده وجود دارد.

مرور پژوهش‌های پیشین

- **AirHopper:** استخراج داده‌ها از طریق امواج FM تولید شده با استفاده از کارت گرافیک
- **USBee:** تولید سیگنال رادیویی از طریق تغییر ولتاژ در باس USB بدون هیچگونه سخت افزار اضافی
- **BitWhisper:** انتقال داده با حرارت میان دو سیستم کامپیوتری مجاور از طریق دمای پردازنده
- **PowerHammer:** ارسال اطلاعات از طریق تغییر در مصرف برق سیستم
- **Fansmitter:** تبدیل فن کامپیوتر به فرستنده صوتی برای ارسال داده
- **MAGNETO:** استفاده از نوسانات مغناطیسی حافظه برای ارسال اطلاعات
- **ODINI:** استخراج داده از طریق نوسانات مغناطیسی تولید شده توسط CPU

طبقه‌بندی روش‌های حمله کانال جانبی در سامانه‌های air-gap

نوع کانال جانبی	مثال پژوهشی	توضیح مختصر
الکترومغناطیسی (EM)	AirHopper, USBee, RAMBO	تولید امواج رادیویی/الکترومغناطیسی حاصل از USB، GPU یا RAM
حرارتی (Thermal)	BitWhisper	تغییر حرارتی CPU برای برقراری ارتباط بین دو سیستم نزدیک
صوتی (Acoustic)	Fansmitter	استفاده از صدای فن یا اسپیکر برای نشت داده ها
الکتریکی (Power-based)	PowerHammer	انتقال داده از طریق تغییر در بار الکتریکی سیستم در کابل تغذیه
مغناطیسی (Magnetic)	MAGNETO, ODINI	ارسال داده با نوسات میدان مغناطیسی CPU یا DRAM

بررسی متدولوژی حمله RAMBO

حمله RAMBO نشان می‌دهد که حافظه RAM می‌تواند به عنوان منبع تولید امواج رادیویی عمل کند. این حمله شامل مراحل زیر است:

- کنترل الگوهای دسترسی به RAM توسط بدافزار برای ایجاد تغییرات قابل پیش‌بینی در مصرف برق.
- رمزگذاری داده‌ها از طریق روش‌های خاص مانند B-FSK برای افزایش نرخ انتقال و کاهش نویز.
- ایجاد نوسانات الکترومغناطیسی ناشی از فعالیت‌های خاص حافظه.
- گیرنده خارجی مثل SDR (Software Defined Radio) که قادر به دریافت این امواج و استخراج داده‌های نهفته در آن‌ها است.

مقایسه حمله RAMBO با سایر حملات مشابه

ویژگی‌ها	RAMBO	AirHopper	PowerHammer	Fansmitter
نوع سیگنال	رادیویی (EM)	رادیویی (FM)	برق AC	صوتی
سخت‌افزار لازم	فقط RAM	کارت گرافیک	کنترل منبع تغذیه	فن سیستم
نرخ انتقال داده	تا چند بیت در ثانیه	مشابه	کمتر	پایین‌تر
قابلیت شناسایی	نسبتاً کم	متوسط	بالا	بالا

بررسی Proof of Concept

- سیستم قربانی یک کامپیوتر air-gap می‌باشد.
- گیرنده سیگنال یک آنتن متصل به SDR بود که تا فاصله چند متری داده‌ها را با موفقیت دریافت نمود.
- داده‌هایی مانند کلید رمزنگاری، رشته‌های متن و حتی دستورات ساده منتقل شدند.
- از رمزگذاری نوع B-FSK برای جداسازی بیت‌ها از نویز استفاده شده بود.

نتایج و یافته‌ها

- سیستم‌های air-gap در برابر مهاجمی با دسترسی فیزیکی اولیه (برای نصب بدافزار) آسیب‌پذیر هستند.
- استفاده از حافظه RAM به‌عنوان فرستنده رادیویی بدون نیاز به سخت‌افزار جانبی امکان‌پذیر است.
- امواج تولیدشده حاصل از نوسانات الکترومغناطیسی RAM قابلیت عبور از موانع معمول اداری را دارند.

محدودیت‌ها

- **نیاز به نصب بدافزار:** بدون دسترسی اولیه، اجرای حمله ممکن نیست.
- **فاصله محدود:** حداکثر چند متر برای انتقال مطمئن.
- **نرخ پایین انتقال داده:** قابل استفاده برای داده‌های کوچک با حجم کم.
- **وجود نویز محیطی:** ممکن است دریافت سیگنال را مختل کند.

روش‌های مقابله

راهکار امنیتی	توضیح مختصر
محدود کردن دسترسی فیزیکی	کاهش احتمال نصب بدافزار در مرحله اول
جداسازی فیزیکی سیستم‌های حساس	نگهداری سیستم‌ها در محیط‌های کنترل‌شده
استفاده از ابزارهای تشخیص ترافیک غیرمعمول در RAM	تشخیص رفتارهای غیرعادی حافظه
استفاده از قفس فارادی	جلوگیری از نشت امواج به بیرون از سیستم
نظارت الکترومغناطیسی محیط	تحلیل فعالیت‌های الکترومغناطیسی و کشف ناهنجاری‌ها

منبع اصلی

Guri, M. et al. “RAMBO: Leaking Secrets from Air-gapped Computers by Spelling Covert Radio Signals from RAM”, [2024].