Practical power analysis attack on an FPGA implementation of AES

انجام عملی حمله‌ی تحلیل توانی بر روی یک پیاده‌سازی از AES بر روی FPGA

امنیت سامانه‌های رمزنگاری همواره یکی از مباحث مورد توجه فعالان حوزه‌ی امنیت بوده‌است. بررسی حملات موفق به این سامانه‌ها نشان می‌دهد که منشأ آسیب‌پذیری در اکثر موارد، نه در مباحث نظری بلکه در پیاده‌سازی الگوریتم‌ها بوده‌است. یکی از قدرتمندترین و در عین حال کم‌هزینه‌ترین حملات انجام‌شده به پیاده‌سازی سامانه‌های رمزنگاری، حملات کانال جانبی هستند. در این حملات با تحلیل اطلاعات جانبی نشت‌شده از پیاده‌سازی الگوریتم‌های رمزنگاری، از سد پیچیدگی محاسباتی عبور کرده و این سیستم‌ها را آسیب‌پذیر می‌کنند.

یکی از اولین حملات کانال جانبی در سال ۹۶ میلادی و با بهره‌گیری از زمان اجرای عملیات رمزنگاری انجام شد. پس از آن، حملات مختلفی برای دست‌یابی به کلید عملیات رمزنگاری ارائه شد که هر یک اطلاعات مختلفی را مورد استفاده قرار می‌دادند. توان مصرفی و تشعشع الکترومغناطیس سیستم در حین انجام عملیات رمزنگاری از مهمترین اطلاعاتی هستند که تحلیل آن‌ها می‌تواند استخراج کلید عملیات رمزنگاری را در پی داشته‌باشد.

در این کارسوق با استفاده از وسایل وابزار مناسب ابتدا به اندازه‌گیری توان مصرفی یک تراشه‌ی FPGA در حین اجرای یک الگوریتم رمزنگاری خواهیم پرداخت و سپس با اعمال روش‌های مختلف کلید عملیات رمزنگاری را از آن‌ها استخراج خواهیم کرد. در نهایت نیز به بررسی اجمالی راهکارهایی خواهیم پرداخت که به کاربستن آن‌ها میزان موفقیت حملات کانال جانبی را کاهش می‌دهد. وسایل مورد استفاده بورد ویژه‌ی ارزیابی حملات کانال جانبی و اسیلوسکوپ دیجیتال با قابلیت نمونه‌برداری بالا هستند.

جلسه	زمان	توضیحات	زمان (دقیقه)
آشنایی با حملات	۹:۳۰ – ۱۰:۳۰	مقدمه‌ای بر حملات فیزیکی	۵۰
		پرسش و پاسخ	۱۰
استراحت اول	۱۰:۳۰-۱۰:۵۰	-	۲۰
حملات مقدماتی	۱۰:۵۰-۱۲:۰۰	آشنایی اجمالی حملات تحلیل توانی	۲۰
		معرفی setup	۱۰
		انجام تحلیل توانی تفاضلی	۲۰
		پرسش و پاسخ	۲۰
نماز و ناهار	۱۲:۰۰ – ۱۳:۴۰	-	۱۰۰
حملات پیشرفته	۱۳:۴۰ – ۱۴:۴۰	انجام تحلیل توانی هم‌بستگی	۲۰
		انجام حمله‌ی الگویی	۳۰
		پرسش و پاسخ	۱۰
استراحت دوم	۱۴:۴۰ – ۱۵:۰۰	-	۲۰
مقابله ها	۱۵:۰۰ – ۱۶:۳۰	مقدمه‌ای بر روش‌های مقابله	۲۰
		معرفی روش MDPL	۲۰
		انجام حمله‌ی ناموفق به پیاده‌سازی این روش	۲۰
		پرسش و پاسخ	۳۰