به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

نگاهی اجمالی بر حملات کانال جانبی و روش‌های مقابله

An Overview of Side Channel Attacks and Countermeasures

محمدحسین فرزام

زمان: شنبه ۶ تیرماه ۱۳۹۴ ساعت ۹:۱۵

مکان: دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف، طبقه چهارم، سالن خوارزمی (۴۰۴)

امنیت سامانه‌های رمزنگاری همواره یکی از مباحث مورد توجه فعالان حوزه‌ی امنیت بوده است. بررسی حملات موفق به این سامانه‌ها نشان می‌دهد که منشأ آسیب‌پذیری در اکثر موارد، نه در مباحث نظری بلکه در پیاده‌سازی الگوریتم‌ها بوده است. 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.

اولین حمله‌ی کانال جانبی موفق در سال ۹۶ میلادی بر روی الگوریتم RSA 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. راهکارهای متعددی نیز برای مقابله با این حملات ارائه‌شده‌است. اکثر این راهکارها سعی در کاهش هم‌بستگی موجود بین اطلاعات جانبی قابل نشت و داده‌های محرمانه سیستم مانند کلید رمزنگاری دارند. در این ارائه سعی خواهدشد به بررسی اجمالی برخی از انواع حملات کانال جانبی و راهکارهای برجسته‌ی مقابله با آن‌ها پرداخته‌شود.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.