به نام خدا

جلسه ارائه هفتگی آزمایشگاه امنیت داده و شبکه


# اجرای حملات کانال جانبی به شماهای مشبکه‌مبنای پیاده‌سازی شده بر روی کارت هوشمند

# Mounting Side-Channel Attacks to Lattice-Based Schemes Implemented on Smart Cards

احمد بورقانی فراهانی

زمان: شنبه ۱۵ آبان ماه ۱۳۹۵، ساعت ۱۵: ۹ صبح

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

حملات کانال جانبی یکی از مهمترین حملات وارد بر سامانه‌های امنیتی می‌باشد که ضعف در پیاده‌سازی یک الگوریتم رمزنگاری را هدف قرار می‌دهد. پیاده‌سازی ساده هر الگوریتم رمزنگاری، حتی در صورتی که از لحاظ تئوری بسیار امن باشد، به احتمال زیاد منجر به نشت اطلاعات از طریق اندازه‌گیری زمان اجرا، توان مصرفی دستگاه، الگوی استفاده از کَش پردازنده، و غیره می‌گردد. در این ارائه، به موضوع حمله کانال جانبی بر روی شماهای رمزنگاری مشبکه‌مبنا می‌پردازیم. این موضوع پژوهشی، به دلیل اینکه به تازگی وارد حوزه کاربردی شده است، از این منظر بسیار مورد توجه می‌باشد و چالش‌های متنوعی در خصوص حمله موفق کانال جانبی به شماهای مبتنی بر مشبکه و همچنین روش‌های مقابله با آنها وجود دارد. در این ارائه همچنین، نتایج یک حمله موفق به پیاده‌سازی یک الگوریتم رمزگذاری و احراز هویت مشبکه‌مبنا بر روی کارت‌های هوشمند ارائه خواهد گردید.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.