به نام خدا

جلسه سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

سطح امنیت ترافیک رمزشده در مقابله با تحلیلگرهای ترافیکی یادگیری-مبنا

The Security Level of Encrypted Traffic Against Learning-Based Classifiers

فرزام فانی طبسی

زمان: یک شنبه ۲۵ آبان ماه ۱۳۹۳ ساعت ۱۵: ۴ عصر

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

از متداول‌ترین روش‌های حفظ محرمانگی و حریم خصوصی در بستر تبادلات ترافیک شبکه، رمزنگاری بسته‌های ارسالی می‌باشد. با استفاده از سازوکارهای رمزنگاری، هر گره شبکه می‌تواند محتویات بسته‌های ارسالی خود را از دید مهاجمان پنهان کند. با این وجود عموم روندهای رمزنگاری توانایی پنهان‌سازی خصوصیات رفتاری ترافیک آشکار از قبیل متوسط زمان رفت و برگشت بسته‌ها، اندازه ریزدانه‌ی بسته‌های ارسالی و دریافتی و همچنین جهت تردد هر بسته، را ندارند. تحلیل‌گرهای ترافیکی یادگیری-مبنا از همین نقطه ضعف روش‌های سنتی رمزنگاری استفاده کرده و قابلیت این را دارند که با استفاده از همین خصوصیات رفتاری، اطلاعاتی در مورد ترافیک رمزشده افشا کنند که به نقض حریم خصوصی و محرمانگی اطلاعات کاربر منجر می‌شود. در همین زمینه تحقیقات اخیر باعث بوجود آمدن تحلیل‌گرهایی شده‌اند که می‌توانند حتی در برابر ترافیک در حال عبور از داخل یک تونل رمزشده، با دقتی بالای ۹۰٪ مقصد ترافیک ارسالی و یا فرستنده‌ی آن جریان ترافیک را شناسایی کنند. در این مطالعه سعی شده است تا ابتدا به معرفی معروف‌ترین این تحلیل‌گرها پرداخته شود و سپس چندین مورد از روشهای پیشنهادی برای مقابلع با این تحلیل‌گر ها بررسی و نتایج از دو دیدگاه سربار ترافیکی و سربار زمانی مورد بحث قرار گیرند. همچنین در انتها روش پیشنهادی خود ارایه دهنده نیز معرفی و تحلیل خواهد شد.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.