

به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه



# یک شیوه‌ی واکاوی ترافیک رمز شده در شبکه‌ی LTE

## An Encrypted Traffic Analysis Method in LTE Network

زینب صالحی مزده

زمان: شنبه ۱۸ دی ماه ۱۳۹۵ ساعت ۹:۱۵

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

با ظهور تکنولوژی (LTE) Long Term Evaluation، استفاده از سرویس‌های مبتنی بر LTE به طور فزاینده‌ای رشد داشته است. به منظور اجرای درست وظایف مدیریت شبکه مانند مدیریت پهنای باند مصرفی، امنیت و حصول اطمینان از کیفیت خدمات سرویس، ارائه‌ی یک طبقه‌بندی کارآمد از ترافیک شبکه‌ی LTE ضروری است. در این تحقیق نیاز به بررسی ترافیک سرویس‌های مختلف بر روی شبکه‌ی LTE وجود دارد، که بدین منظور اسکایپ مورد مطالعه قرار می‌گیرد؛ زیرا در چند سال اخیر، اسکایپ دارای محبوبیت زیاد و به عنوان بهترین انتخاب برای استفاده از سرویس VoIP شناخته شده است، از طرفی ارائه‌ی دامنه‌ی گسترده‌ای از خدمات شامل تماس تلفنی، Skype Out، پیام‌های فوری، تبادل فایل، ویدئو کنفرانس و ... بیش از پیش به شهرت آن در بین همگان افزوده است. اسکایپ یک پروتکل اختصاصی بر مبنای معماری نظیر-به-نظیر دارد که از رمزنگاری در ارتباطات انتها به انتها استفاده می‌کند و شیوه‌هایی به منظور جلوگیری از مهندسی معکوس پروتکل اختصاصی خود را دارد. افزون بر این‌ها، در اسکایپ به دلیل ترکیب رمز کردن تمامی ارتباطات و انتشار درگاه به صورت پویا، شناسایی جریان‌های آن را تبدیل به یک عمل چالشی کرده است و شیوه‌های سنتی تحلیل ترافیک را در مورد آن ناکارآمد می‌کند. به همین منظور در این پژوهش، تلاش خواهد شد روشی عملیاتی برای واکاوی ترافیک رمز شده اسکایپ تحت شبکه‌ی LTE ارائه شود.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.