به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

طبقه‌بندی ترافیک رمزشده

Encrypted Traffic Classification

سعید شهراب

زمان: شنبه ۱۴ شهریور ماه ۱۳۹۴ ساعت ۱۵:۹

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

ده‌بندی ترافیک می‌تواند به حل برخی مشکلات در مدیریت شبکه کمک کند. اپراتورهای شبکه برای تعرفه‌گذاری ارائه خدمات خود نیازمند اطلاع از کلیات داده‌های عبور داده شده از شبکه هستند. رده‌بندی ترافیک، می‌تواند این اطلاعات را در اختیار آن‌ها قرار دهد و به همین دلیل می‌تواند هسته‌ی اصلی بسیاری از خدمات ارائه شده باشد. روش‌های مرسوم رده‌بندی ترافیک، بر بازرسی درگاه بسته‌های TCP و UDP یا شناسایی امضای پروتکل‌ها بر اساس محتوای بسته‌ها تکیه دارد. اما این روش‌ها با محدودیت‌های جدی روبرو هستند. در صورتی که یک جریان از درگاه شناخته شده‌ای استفاده نکند و یا سرویسی بر روی درگاهی غیرمعمول ارائه شود روش‌های مبتنی بر درگاه در رده‌بندی جریان دچار مشکل خواهد شد. برای کاهش وابستگی به درگاه، رده‌بندی مبتنی بر محتوای بسته با مشاهده‌ی مقداری از داده‌های تبادل شده در جریان سعی می‌کند پروتکل را شناسایی کند. اما با توجه به اینکه بسیاری از ارتباطات بعد از لایه‌ی انتقال در شبکه به صورت رمز شده هستند. امکان استفاده از رده‌بندی مبتنی بر محتوای بسته وجود ندارد. علاوه بر این در صورتی که کاربران ترافیک خود را از تونلی رمزشده عبور دهند روش‌های مرسوم رده‌بندی ترافیک به طور کامل کارایی خود را از دست می‌دهند. روش‌های جدید رده‌بندی ترافیک، بر خلاف روش‌های مرسوم، از محتویات بسته برای رده‌بندی استفاده نمی‌کنند بلکه بر مشخصات آماری ترافیک نظیر طول بسته‌ها، جهت انتقال بسته و تعداد بسته‌ها تکیه دارند. این روش‌ها اطلاعات آماری را استخراج و با کمک روش‌های داده کاوی و یادگیری ماشین ترافیک شبکه را دسته‌بندی می‌کنند. در این ارائه مروری بر روی پژوهش‌های انجام شده در این زمینه انجام خواهیم داد، و به صورت مختصر رویکردهای مختلف را بررسی می‌کنیم و به ذکر برخی از چالش‌های این نوع طبقه‌بندی می‌پردازیم.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.