به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

اعمال خط‌مشی امنیتی رفتار-رانه بر روی شبکه‌های پهن‌باند

Behavior-Driven Security Policy Enforcement on High Bandwidth Networks

مرتضی نوفرستی

زمان: شنبه ۲۴ بهمن ماه ۱۳۹۴ ساعت ۹:۱۵

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

حجم زیاد و سرعت بالای ترافیک شبکه‌های پهن‌باند، باعث ایجاد نیازمندی‌های جدید امنیتی در این شبکه‌ها شده است. دنبال‌کردن تغییرات شبکه، کنترل نوفه، یک‌بار پردازشی بودن، و محدودیت‌های تأخیر و حافظه چالش‌های اصلی اِعمال خط‌مشی امنیتی در شبکه‌های پهن‌باند هستند. با در نظر گرفتن این چالش‌ها، طراحی و تولید سامانه‌های نوین برای پاسخگویی به نیازمندی‌های جدید امنیتی امری ضروری به نظر می‌رسد. این پیشنهاد پژوهشی با در نظر داشتن چالش‌های مذکور، یک چارچوب برای اعمال خط‌مشی امنیتی در دولایه‌ی سازوکار و خط‌مشی ارایه می‌کند. در لایه‌ی سازوکار، اطلاعات موجود در سرآیند و بدنه‌ی بسته‌های ترافیک عبوری استخراج شده و بر مبنای آن جویبار رویدادها تولید می‌شود. این جویبار رویدادها در لایه‌ی خط‌مشی برای تشخیص رفتار کاربران و اعمال خط‌مشی‌های امنیتی تحلیل می‌گردد. در این لایه، مفهومی به نام ابررویداد بر مبنای خاصیت محلی بودن رویدادها تعریف می‌شود. ارتباط‌های بین ابررویدادها برای استخراج رفتارهای موجود در شبکه استفاده می‌شوند. ارزیابی اولیه‌ی ما از طریق شبیه‌سازی نشان دهنده‌ی دقت و کارایی بالای چارچوب پیشنهادی برای تولید سامانه‌های امنیت پهن باند است

.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.