به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

همبسته سازی هشدارهای حجیم به منظور کشف الگوی حمله‌های پرتکرار

High Volume Alert Correlation for Frequent Attack Pattern Mining

زهرا حسام نیر

زمان: شنبه ۱۷ آذر ماه ۱۳۹۷ ساعت ۹:۱۵

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

با افزایش روزافزون استفاده‌ی افراد از شبکه‌های کامپیوتری، با چالش‌هایی روبه‌رو هستیم. از جمله این چالش‌ها تامین امنیت شبکه‌های کامپیوتری می‌باشد. با تولید حجم عظیم رویدادها به وسیله‌ی سیستم‌های تشخیص نفوذ سطح-پایین، مدیریت هشدارها و تشخیص نفوذ احتمالی به عنوان یک چالش پیش‌رو مطرح است. تحلیل دستی حجم عظیم هشدارهای خام، بسیار وقت‌گیر، نادقیق و در مواردی ناممکن است. یک پاسخ مناسب برای این مسئله همبسته‌سازی هشدارها به صورت خودکار است. به منظور ارائه دید سطح بالاتری از فرآیندهای شبکه، علاوه بر شباهت‌یابی و کشف رابطه علیت بین هشدارهای خام، پنجره زمانی بزرگی از هشدارها در نظر گرفته می‌شود و با رویکرد برون‌خط به دنبال راه‌کاری برای کاوش در حجم عظیم هشدارها به منظور یافتن الگوی حمله‌های پرتکرار هستیم.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.