به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

همبسته سازی رویدادهای حجیم به منظور کشف الگوهای حملات پر تکرار

High Volume Event Correlation for Frequent Attack Pattern Mining

زهرا حسام نیر

زمان: شنبه ۱۶ دی ماه ۱۳۹۶ 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 سیستم های تشخیص نفوذ سطح-پایین، مدیریت هشدارها و تشخیص نفوذ احتمالی به عنوان یک چالش پیش رو مطرح است. تحلیل دستی حجم عظیم رویدادهای خام، بسیار وقت گیر، نادقیق و در مواردی ناممکن است. یک پاسخ مناسب برای این مسئله همبسته سازی هشدار ها به صورت اتوماتیک می باشد. به منظور ارائه دید سطح بالاتری از فرآیندهای شبکه، علاوه بر شباهت یابی و کشف رابطه علیت بین هشدارهای خام، پنجره زمانی بزرگی از رویدادها در نظر گرفته می شود و با رویکرد برون خط به دنبال راهکاری برای کاوش در حجم عظیم رویدادها به منظور یافتن الگوی حمله های پر تکرار هستیم.

شرکت در این جلسه برای تمامی علاقمندان آزاد است.