به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

همبسته‌سازی رویدادهای حجیم جهت کشف حملات بلندمدت

High Volume Event Correlation for Long-term Attack Detection

نیلوفر مخزون

زمان: شنبه ۶ آبان ماه ۱۳۹۶ ساعت 9:15

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

امروزه با پیشرفت تکنولوژی و گسترش سیستم‌های اطلاعاتی در سازمان‌های مهم دولتی، امنیت اطلاعات به حساس‌ترین مسئله روز تبدیل گشته است. با ابزارهای فعلی موجود در بازار، تشخیص حملات تک‌مرحله‌ای و شناخته‌شده تا حد زیادی امکان پذیر است؛ اما وقتی این حملات ساده با یکدیگر ترکیب می‌شوند و با سناریوهای پیچیده، سیستمی را هدف قرار می‌دهند تشخیص آن‌ها به سادگی نخواهد بود. اگر صرفا دنباله‌ای از این حملات شناخته شده را داشتیم می‌توانستیم با استفاده از الگوریتم‌های همبسته‌سازی فعلی، سناریوی حمله را پیگیری و کشف کنیم؛ اما مسئله وقتی پیچیده می‌شود که سرعت اجرای گام‌های سناریوی حمله کم باشد و گام‌های ناشناخته و ابتکاری نیز به آن افزوده گردد. سیستم‌های فعلی توانایی تشخیص حرکات توزیع‌شده در سامانه یا حرکت در سطح پایین و آهسته با مدت طولانی را ندارند؛ زیرا کشف این حملات نیاز به تحلیلی عمیق در حجم عظیمی از رویدادهای سیستم و شبکه در بلندمدت دارد. از نمونه‌های مطرح این حملات چند مرحله‌ای و بلندمدت، تهدیدات مانای پیشرفته هستند که عمده هدف آن‌ها، سازمان‌های مهم در کشور است. در سال‌های اخیر فعالیت‌های زیادی جهت کشف این دسته از حملات صورت گرفته است. در این ارائه به بررسی چرخه حیات حملات مانای پیشرفته و برخی راهکارهای تشخیص آن‌ها خواهیم پرداخت.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.