به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

تشخیص نقض محرمانگی ناشی از تهدیدات مانای پیشرفته کوتاه‌مدت مبتنی بر همبسته‌سازی جریان داده

Detection of Confidentiality Violation by Short-term Advanced Persistent Threats based on Data Stream Correlation

سید حیدر جوادی

زمان: شنبه ۱۲آبان ماه ۱۳۹۷، ساعت ۹:۱۵

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

حملات مانای پیشرفته با انجام رفتارهای چندمرحله‌ای، سطح پایین و در مواردی آهسته، رفتار مخرب خود را توزیع و پنهان می‌سازند. این حملات پیچیده و پرهزینه بوده و معمولا از سوی نهادهای دولتی به صورت خاص-منظوره طراحی شده و زیرساخت‌های حیاتی کشوری دیگر را هدف قرار می‌دهند. برای تشخیص وجود حملات مانای پیشرفته ناگزیر هستیم رویدادهای صورت گرفته را با ریزدانگی بالا و در کنار یکدیگر پویش کنیم. چرا که اتکا به هشدارهای سیستم‌های امنیتی عمومی و سپس همبسته‌سازی آنها، به علت از دست رفتن اطلاعات رویدادها و در نظر گرفته نشدن بعضی از روابط، ممکن است رفتار مخرب شکل گرفته را آشکار نسازد. همین امر منجر به تولید حجم عظیم رویدادها و روابط بین آن‌ها می‌گردد. در این سخنرانی، با بهره‌گیری از تکنیک‌های پردازش بی‌درنگ داده حجیم راهکاری برای رهگیری لحظه‌ای دسترسی‌های صریح و ضمنی صورت گرفته از سوی عامل‌های درگیر سازمان در نتیجه تشخیص بی‌درنگ نقض سیاست‌های محرمانگی سازمان از سوی حملات مانای پیشرفته که در کوتاه مدت بردار حمله خود را اجرا می‌کنند، شرح داده خواهد شد.

شرکت در این جلسه برای تمامی علاقه‌مندان آزاد است.