به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

همبسته‌سازی مبتنی بر معناجهت شناسایی حملات مانای پیشرفته‌ی ترکیبی و سطح پایین

امیر محمدزاده لاجوردی

زمان: شنبه ۷ مردادماه ۱۳۹۶ ساعت ۹:۱۵

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

بدافزارهای هدفمند و پیچیده همانند حملات مانای پیشرفته، با استفاده از رفتارهای چندمرحله‌ای، توزیع‌شده، ترکیبی، و سطح پایین، خط‌مشی‌های امنیتی سیستم را نقض می‌کنند. به دلیل آنکه سیستم‌های تشخیص نفوذ و همبسته‌سازی هشدار، رویدادهای سطح پایین سیستم‌عامل را با رویدادهای سطح شبکه همبسته نمی‌کنند و از همبسته‌سازی هشدار به‌جای همبسته‌سازی رویداد استفاده می‌شود، حمله‌کننده با استفاده از رویدادهای ترکیبی و سطح پایین بردار حمله را توزیع‌کرده و رفتار خود را پنهان می‌سازد.

در این ارائه قصد داریم به بررسی نحوه رفتار این حملات و ارائه راهکاری جهت شناسایی آن‌ها بپردازیم. در این روش از رهگیری عمیق رویدادها، و همبسته‌سازی رویدادهای شبکه با سیستم‌عامل استفاده می‌شود. رفتارهای مخرب، به ویژه نقض ضمنی خط مشی امنیتی، با استفاده از استنتاج مبتنی بر روابط بین رویدادها و خط‌مشی‌های امنیتی شناسایی می‌گردد. همچنین انتقال جریان اطلاعات بین عامل‌ها بر اساس هستی‌شناسی سیستم‌عامل و با هدف شناسایی بردارهای حمله توزیع شده صورت می‌گیرد. آزمون روش پیشنهادی بر روی سناریوی ۱۲ تهدید مانای پیشرفته نشان‌دهنده کارایی راهکار پیشنهادی است.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.

سوابق سخنران : www.ce.sharif.edu/~lajevardi