به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

تشخیص جریان‌های بدخواه در شبکه بر اساس خصوصیت‌های رفتاری کاربران

ابوالفضل زرگر

زمان: شنبه ۱۳ شهریور ماه ۱۳۹۵ ساعت ۹:۱۵

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

امروزه سازمان‌های بزرگ باوجود هزینه‌های فراوان برای ایمن‌سازی در برابر مهاجمان خارجی، از خویش‌تهدیدها رنج می‌برند. دسترسی و شناخت بالای خودی‌ها نسبت به منابع سازمان در این تهدیدات، می‌تواند با هزینه کم‌تر، آسیب‌های هدفمندتر و جدی‌تری به سازمان وارد کند. در این پایان‌نامه، راهکاری برای تشخیص این‌گونه تهدیدات ارائه خواهیم داد. این راهکار، با فرض حداقل بلوغ امنیتی برای سازمان، سعی می‌کند که در انواع محیط‌ها و سناریوها با کمترین تنظیمات اولیه، دسته‌ای از خویش‌تهدیدها را از طریق نمایه‌بندی رفتار کاربران شناسایی کند. دو نمونه از تهدیدات مدنظر در شرایط عادی، توسط راهکار پیشنهادی تشخیص داده شد. از طرفی دو سری دادگان از همین تهدیدات در شرایط پیچیده تهیه شد و با تحلیل نتایج آن، چالش‌های راهکار پیشنهادی به همراه راهکارهای آن‌ها استخراج شد. با تشخیص این سناریوهای نمونه، می‌توان انتظار داشت که سناریوهای مشابه زیادی در کاربردها و محیط‌های مختلف قابل‌تشخیص باشد.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.