به نام خدا

جلسه ارائه هفتگی آزمایشگاه امنیت داده و شبکه

همبسته‌سازی هشدار در سامانه اخطار زودهنگام

Alert Correlation in Early Warning System

علی احمدیان رمکی

زمان: **شنبه ۶ مهر، ساعت ۹ صبح**

مکان: **دانشگاه صنعتی شریف، دانشکده مهندسی کامپیوتر، طبقه پنجم، آزمایشگاه امنیت داده و شبکه**

امروزه این نتیجه حاصل شده است که راه‌حل‌های پیش‌گیرانه به‌تنهایی در مورد امنیت اطلاعات کافی نیست. بنابراین نیاز به روش‌های واکنشی است که حملات و تهدیدات را به موقع شناسایی کنند. "*سیستم‌های اخطار زودهنگام*" راهکاری واکنشی در مقابل تهدیدات امنیتی هستند. این سیستم‌ها مکمل "*سیستم‌های تشخیص نفوذ*" هستند که هدف اصلی آن‌ها تشخیص زودهنگام رفتارهای بالقوه سیستم، ارزیابی و پیش‌بینی محدوده فعالیت‌های بدخواهانه و در نهایت نیز اعمال واکنشی درخور در برابر هرگونه رخداد امنیتی قابل تشخیص است. یکی از فرآیندهای مهم در این سامانه‌ها، تحلیل و همبسته‌سازی هشدارهای دریافتی از حس‌گرهاست. "*همبسته‌سازی هشدار*" یک فرآیند تحلیلی است که هشدارهای تولید شده توسط حس‌گرهای امنیتی را به‌عنوان ورودی دریافت می‌کند و گزارش‌های فشرده‌ای از وضعیت امنیتی شبکه تحت نظارت ارائه می‌دهد. در این ارائه ضمن مرور مفاهیم سیستم اخطار زودهنگام، به اهمیت فرآیند همبسته‌سازی در این سامانه‌ها جهت دستیابی به یک تصویر کلی از وضعیت امنیتی شبکه خواهیم پرداخت. علاوه بر آن ضمن مرور سیستم‌های اخطار زودهنگام معرفی‌شده در حوزه امنیت اطلاعات، روش‌های همبسته‌سازی هشدار را دسته‌بندی خواهیم نمود. در ادامه ضمن معرفی یک چارچوب پیشنهادی برای همبسته‌سازی هشدارها جهت تشخیص "*سناریوهای حملات شناخته شده و حملات ناشناخته* جدید"، چگونگی پیش‌بینی گام‌های بعدی یک حمله چندمرحله‌ای را ارائه خواهیم داد.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.