به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

رویکردی جامع در همبسته‌سازی مبتنی بر شباهت

A Comprehensive Approach to Similarity-Based Alert Correlation

احمد سپاهی

زمان: شنبه ۱۶ آذرماه ۱۳۹۲ ساعت ۹ صبح

مکان: دانشکده مهندسی کامپیوتر، طبقه پنجم، آزمایشگاه امنیت داده و شبکه

در پاسخ به حملاتی که به شبکه‌های کامپیوتری می‌شود، مدیران شبکه بطور فزاینده‌ای از سامانه‌های تشخیص نفوذ استفاده می‌کنند. سامانه‌های تشخیص نفوذ با تحلیل اطلاعات بدست آمده از فعالیت‌های رایانه‌ها و شبکه‌ها، در جست‌وجوی شواهدی از رفتار مخرب هستند. این سامانه‌ها معمولا هشدارهای زیادی تولید می‌کنند که مدیریت این حجم انبوه از هشدارها بسیار دشوار و گاه غیر ممکن است. مشکل دیگر سامانه‌های تشخیص نفوذ، وجود هشدارهای مثبت غلط، منفی غلط، و مثبت نامربوط است. بهره‌گیری از چند سامانه تشخیص نفوذ بطور همزمان به منظور پوشش نقاط ضعف یکدیگر، باعث افزایش حجم هشدارها و کاهش کیفیت آنها می‌گردد. به منظور رفع این مشکل‌ها، سامانه‌های همبسته‌ساز هشدار پیشنهاد شده‌اند. همبسته‌ساز هشدار سامانه‌ای است که هشدارها را از سامانه‌های تشخیص نفوذ ناهمگون دریافت و تعداد هشدارهای اشتباه را کاهش می‌دهد. همچنین الگوهای سطح بالا را تشخیص داده، حالت آتی حمله را پیش بینی می‌نماید و علت اصلی حمله را نمایان می‌سازد. الگوریتم‌های همبسته‌ساز هشدار در سه دسته طبقه‌بندی می‌گردند که عبارتند از: مبتنی بر شباهت، مبتنی بر دانش، و الگوریتم‌های آماری. در این سخنرانی، هر یک از این روش‌ها به اختصار توضیح داده می‌شوند. سپس رویکردی جامع برای همبسته‌سازی مبتنی بر شباهت، ارائه شده و اجزای آن شرح داده می‌شوند.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.