به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

تشخیص تهاجم با استفاده از داده‌کاوی

Intrusion Detection by Data Mining

محسن زندی

زمان: شنبه ۳۰ فروردین ماه ۱۳۹۳ ساعت ۳ عصر

مکان: دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف، طبقه چهارم، سالن ۴۰۴

سیستم‌های تشخیص‌نفوذی که بر اساس داده‌کاوی طراحی شده‌اند، در شبکه‌های بزرگ بدلیل تولید هشدارهای اشتباه در زمینه حملات به شبکه، عملاً دارای کاربرد نیستند. به همین دلیل در سیستم‌های تشخیص نفوذ تجاری عملاً از داده کاوی استفاده نمی‌کنند. در سیستم‌های تجاری از الگو و امضای حملات شناخته شده استفاده می‌گردد. اینگونه امضاها ایستا بوده، یعنی امضا و الگوی هر حمله پس از مشاهده رفتار آن حمله و ثبت داده‌های مربوط به آن با تحلیل‌هایی که بر روی داده‌ها صورت می‌گیرد، تهیه می‌گردد، بدینوسیله سیستم در آینده به راحتی آن حمله را خواهد شناخت و جلوی نفوذ و حمله به شبکه را خواهد گرفت. با توجه به اینکه اخیراً در تحلیل بر روی داده‌ها جهت استخراج امضا از داده کاوی استفاده می‌گردد، در این سخنرانی تلاش می‌شود تا استفاده از داده‌کاوی در تشخیص تهاجم مورد بحث و بررسی قرار گیرد.

.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.

سوابق سخنران:

محسن زندی

مدیرعامل شرکت مرزگستران فناوری

کارشناس ارشد مدیریت اطلاعات - فارغ‌التحصیل سال ۱۳۸۵

مجری، همکار و ناظر بیش از ۵۰ پروژه فناوری اطلاعات در سطح کشور

۱۰ سال سابقه تدریس، تحقیق و پژوهش در دانشگاه صنعتی مالك اشتر