به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

مدل‌سازی و تحلیل نوع‌مبنای پروتکل‌های تصدیق اصالت با وجود حمله‌های داخلی

Type-based Modeling and Analysis of Authentication in the Presence of Insider Attacks Protocols

دکتر بهنام ستارزاده

زمان: شنبه ۱ آبان ماه ۱۳۹۵ ساعت ۹:۱۵

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

روش نوع‌مبنا یکی از روش‌های موفق در تحلیل پروتکل‌های امنیتی است. از مزایای این روش می‌توان به سرعت بالا، مقیاس‌پذیری، پایان‌پذیری، و امکان خودکارسازی تحلیل اشاره کرد. نیازمندی‌های امنیتی و فرضیات صورت گرفته در مورد توانایی‌های مهاجمان دو پارامتر اصلی هستند که طراحی روش تحلیل نوع‌مبنا را تحت تاثیر قرار می‌دهند. در این ارائه، به منظور رفع کاستی‌های این حوزه، یک روش نوع‌مبنا برای تحلیل خودکار پروتکل‌های تصدیق اصالت در حضور مهاجمان داخلی شرح داده می‌شود. این روش درستی‌سنجی نیازمندی توافق یک‌به‌یک را امکان‌پذیر می‌سازد. این نیازمندی بالاترین سطح امنیتی قابل دستیابی در پروتکل‌های تصدیق اصالت است.

معرفی سخنران: دکتر بهنام ستارزاده در حال در حال حاضر پژوهشگر پژوهشکده پارسا شریف هستند. ایشان مدرک دکتری خود را در رشته مهندسی کامپیوتر (نرم افزار) از دانشگاه صنعتی امیرکبیر و مدرک کارشناسی و کارشناسی ارشد خود را از دانشگاه صنعتی شریف اخذ کرده‌اند. ایشان به موازات تحصیل خود، بیش از ۱۰ سال سابقه فعالیت فنی و اجرایی در زمینه امنیت پایگاه داده، کنترل‌دستری، امنیت شبکه، پروتکل‌های امنیتی، رمزنگاری، تحلیل بدافزار و ... داشته‌اند.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.