به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

طراحی و پیاده‌سازی یک روش تحلیل مبتنی بر رفتار به منظور کشف بدافزارها

Design and Implementation of a new Behavior-Based Analysis Method for Malware Detection

امیر محمدزاده لاجوردی

زمان: شنبه ۲۷ اردیبهشت ماه ۱۳۹۳ ساعت ۳ عصر

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

در این سمینار روشی جهت تحلیل و شناسایی بدافزار در سه فاز ارائه می‌گردد تا معایب روش‌های قبل را برطرف سازد. فاز اول طراحی یک سیستم رهگیری رفتار نرم‌افزار در سه سطح Hypervsior ماشین مجازی، سطح هسته و سطح کاربر است تا بتواند اطلاعات کامل و جامعی از رفتار نرم‌افزار استخراج نماید. در فاز دوم بر اساس استخراج ویژگی‌های مخرب و سالم در کدهای بدخواه و بی‌خطر عمل شناسایی ماهیتِ نرم‌افزار در حال اجرا انجام می‌گردد. این شناسایی بوسیله‌ی دنباله‌ی وابستگیِ معنایی بین فراخوانی‌های سیستمی صورت می‌گیرد. این دنباله بر اساس استخراج وابستگی کنترلی و وابستگی داده‌ای بین فراخوانی‌های سیستمی استخراج می‌گردد. یک چالش اصلی در تحلیل رفتاری بدافزار، نیاز به اجرای آن بر روی سیستم‌عامل میزبان است. بنابراین در فاز آخر یک محیط امن در دو سمت کاربر و سرویس دهنده ارائه می‌گردد. این محیط امن با استفاده از مجازی‌سازیِ درخواست‌های ارائه‌شده توسط بدافزار به سیستم‌عامل، از وارد شدن آسیب به سیستم جلوگیری می‌نماید. در نهایت نشان داده خواهد شد که این محیط دارای سربار بسیار کم و عمق تحلیل زیادی نسبت به روش‌های موجود دیگر است.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.