به نام خدا

جلسه‌ی سخن‌رانی هفتگی آزمایشگاه امنیت داده و شبکه

مروری بر راهکارهای نوین تشخیص بدافزار در سیستم عامل اندروید

A survey on modern malware detection approaches in Android OS

مجید صالحی

زمان: شنبه ۲۳ مردادماه ۱۳۹۵ ساعت ۹:۱۵

مکان: دانشکده‌ی مهندسی کامپیوتر دانشگاه صنعتی شریف، طبقه‌ی چهار، سالن خوارزمی

امروزه حملات روی سامانه‌های هوشمند به صورت گسترده و با رویکردهای پیچیده‌ای توسط بدافزارنویسان و بعضا دولت‌ها با اهداف مختلفی نظیر بدست آوردن شهرت و مقام، دزدیدن اطلاعات محرمانه، انتقال پول، دزدیدن طرح‌ها و برنامه‌های نظامی سازمان‌ها و کشورها انجام می‌شود. اکثر محصولات امنیتی مانند پویشگرهای بدافزار و محصولات ضد بدافزاری برای تشخیص کد مخرب به دنبال امضاء و دنباله‌هایی از بایت‌های خاص می‌گردند. در این میان سازندگان بدافزارها با استفاده از موتورهای چندریختی سعی در تغییر دادن ظاهر بدافزار دارند تا از شناسایی زودرس آن‌ها روی سیستم آلوده جلوگیری به عمل آید. روش‌های عمده‌ای که متخصصین امنیتی، محققین و تحلیل‌گران در شناسایی امضاء بدافزار استفاده می‌کنند روش‌های سنتی تحلیل ایستای کد منبع یا اسمبلی بدافزار با استفاده از تکنیک‌های پیچیده و در بعضی موارد دشوار مهندسی معکوس است. این روش‌ها نه تنها بسیار وقت گیر هستند بلکه نیروی متخصص زیادی را نیز می‌طلبند.

در این ارائه با مروری بر راهکارهای امنیتی موجود و تحلیل معایب و ضعف‌های آن‌ها، اقدام به ارائه یک راهکار پیشنهادی به منظور تحلیل و کشف بدافزارهای اندرویدی با استفاده از اطلاعات رفتاری و پویای برنامه‌های کاربردی خواهیم نمود. روش پیشنهادي سعي در افزايش دقت تشخيص بدافزارها و كاهش سربار تحميل شده به سيستم نسبت به روش‌هاي ديگر دارد.

- شرکت در این جلسه برای همه‌ی دانشجوهای علاقه‌مند آزاد است -