به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

شباهت سنجی مبتنی بر هستی شناسی در بدافزارهای اندرویدی

Ontology-based similarity for android malwares

اسماعیل غلامی

زمان: شنبه ۲۴ فروردین ماه ۱۳۹۸ ساعت ۹:۱۵

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

یکی از راه‌های مقابله با تولید بدافزارهای اندرویدی، شناسایی تولیدکنندگان و منتشرکنندگان آن است. برای مقابله با فعالیت-های سازماندهی شده، شناسایی تمام موارد مربوط به مجموعه افراد ذینفع و فعالیت‌های آن‌ها حائز اهمیت است. معمولا کمپینی برای توزیع بدافزارتوسط تولیدکنندگان آن تشکیل می‌شود. در این کمپین‌ها نسخه‌های مختلف از بدافزارهای اندرویدی ساخته شده و توزیع می‌شوند. لذا تشخیص شباهت بین بدافزارهای مختلف و دسته‌بندی مناسب آنها بر اساس شباهت بین آنها می‌تواند کاربردهای مختلفی در زمینه جرم‌یابی و شناسایی بدافزارها داشته باشد. استفاده از اطلاعات بیرون از بدافزار (ولی مرتبط با آن) و استنتاج مبتنی بر هستی‌شناسی بر اساس آن‌ها می‌تواند منجر به کشف ارتباطات و شباهت‌های مختلف بین بدافزارها شود.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.