بسمه تعالی

☐ دفاع از رساله دکتری ☐ سمینار عمومی (Colloquium)

■ دفاع از پایان‌نامه کارشناسی‌ارشد ☐ سمینار تخصصی (Seminar)

☐ سمینار تخصصی و مشورتی (Informal Seminar)

عنوان : ارائه رویکردی نوین برای کشف بدافزارهای فراریخت

سخنران : امیر نورآذر

چکیده:

حمله‌کنندگان، تکنیک‌های مختلف مبهم‌سازی و تبدیلات حفظ کننده معنا را بکار می‌برند تا ساختار کدهای بدافزار را در هر تکثیر تغییر دهند. این استراتژی‌ها یک بدافزار فراریخت ایجاد می‌کنند که می‌تواند از شناسایی شدن توسط ضد بدافزارها بگریزد. در سال‌های اخیر، فعالیت قابل توجهی در حوزه بدافزار صورت گرفته است و تکنیک‌های مختلفی معرفی شده‌اند. بسیاری از این تکنیک‌ها، بر پایه روش‌های آماری، داده کاوی و یادگیری ماشین فعالیت می‌کنند. در این پایان نامه، ما روش جدید G3MD را برای شناسایی ایستای بدافزارها پیشنهاد می‌کنیم. این روش تلاش می‌کند تا تاثیرات تکنیک‌های مختلف مبهم‌سازی استفاده شده توسط حمله‌کنندگان را رفع کند. به این صورت که الگوهای کدهای یک خانواده از بدافزارهای فراریخت را از گراف‌های حاصل از کدهای عملیاتی بدافزارها استخراج می‌کند.

بطور دقیق‌تر، زیرگراف‌های پرتکرار کدهای عملیاتی، به اصطلاح شبه امضاها، را از خانواده‌های بدافزارهای فراریخت استخراج می‌کند. با توجه به حضور یا عدم حضور هر کدام از این زیرگراف‌ها در هر فایل، یک بردار مشخصه تشکیل می‌شود. سپس این بردارها برای آموزش یک دسته‌بند استفاده می‌شوند. پس از آن، به وسیله این دسته‌بند فایل سالم را از فایل بدافزار فراریخت تشخیص می‌دهیم. ما آزمایشات را بروی چهار خانواده از بدافزارهای فراریخت انجام داده‌ایم که در مطالعات گذشته مورد استفاده قرار گرفته‌اند. این خانواده‌ها عبارتند از ویروس‌های NGVCK، G2 و MPCGEN و کرم‌های MWOR. اغلب روش‌های موجود، از اخطارهای اشتباه و یا عدم موفقیت در مقابل تمام تکنیک‌های مبهم‌سازی رنج می‌برند. دقت تشخیص ۱۰۰ درصد بدافزارهای فراریخت با روش پیشنهادی، اثربخشی این روش را بر روش‌های موجود تایید می‌کند.

کلمات کلیدی: بدافزار فراریخت، گراف‌کاوی، داده کاوی، گراف کدهای عملیاتی، دسته‌بندی و شناسایی بدافزار، مبهم‌سازی

زمان برگزاری: ۹۵/۱۲/۲۸

مکان برگزاری: دانشکده مهندسی و علوم کامپیوتر