دانشگاه شهید بهشتی

دانشکده مهندسی و علوم کامپیوتر

اطلاعیه دفاع

نام دانشجو: **مصطفی جعفری**		**نام استاد راهنما:** **دکتر علیرضا شاملی سندی**
مقطع: کارشناسی ارشد	**رشته: کامپیوتر**	**گرایش: نرم افزار**
نوع دفاع: • **دفاع پروپوزال** □ • **دفاع پایان نامه** ■ • **دفاع رساله دکترا** □		**تاریخ: ۱۴۰۳/۱۱/۳۰** **ساعت: ۱۲:۰۰** **مکان: کلاس ۱۱۷**

عنوان: حملات خصمانه علیه سیستم‌های تشخیص بدافزار اندروید مبتنی بر تحلیل ایستا

داوران خارجی: دکتر بابک صادقیان	**داوران داخلی: دکتر مهران علیدوست نیا**

چکیده: یادگیری ماشین به یکی از ابزارهای کلیدی برای شناسایی بدافزارهای اندروید تبدیل شده است، اما همچنان در برابر حملات خصمانه آسیب‌پذیر است؛ حملاتی که در آن‌ها، تغییرات جزئی می‌توانند به‌سادگی مکانیزم‌های شناسایی را فریب دهند. باوجود پیشرفت‌های قابل‌توجه در تقویت استحکام خصمانه، نبود چارچوب‌های ارزیابی جامع، درک اثربخشی این روش‌ها را محدود کرده است. در این پژوهش، دو نوآوری کلیدی برای بهبود ارزیابی خصمانه در حوزه‌های با محدودیت دودویی ارائه شده است. نخست، تکنیکی به نام گرد کردن دودویی اولویت‌بندی‌شده معرفی شده که پریشیدگی‌های خصمانه پیوسته را به فضاهای دودویی تبدیل می‌کند، در حالی که نرخ موفقیت حمله را در سطح بالایی حفظ کرده و اندازه پریشیدگی را به حداقل می‌رساند. دوم، حمله‌ای نوآورانه با طراحی شده که به‌طور خاص برای حوزه‌های دودویی بهینه شده و با حداقل پریشیدگی، sigma-binary عنوان اثربخشی این رویکرد را تأیید Malscan اهداف خصمانه را محقق می‌سازد. نتایج ارزیابی‌ها بر روی مجموعه‌داده ، PGD و حملات مبتنی بر Mimicry، sigma-zero، CW از روش‌های موجود شامل sigma-binary می‌کند. حمله از نظر نرخ موفقیت و اندازه پریشیدگی پیشی می‌گیرد. تحلیل‌های ما نقاط ضعف قابل‌توجهی را در سیستم‌های با کمتر از ۱۰ تغییر ICNN و +DNN، DLA، KDE دفاعی خصمانه آشکار کرده‌اند. به‌طور خاص، سیستم‌هایی نظیر مشخصه، نرخ موفقیت حمله‌ی بالای ۹۰ درصد را ثبت می‌کنند. این ضعف‌ها حتی در برابر سیستم‌های مستحکم‌تر توانسته در برابر ۱۵ حمله مبتنی PAD-SMA نیز مشاهده می‌شوند. به‌عنوان مثال، اگرچه سیستم دفاعی مستحکم sigma-binary بر گرادیان مقاومت نشان داده و نرخ موفقیت حملات را زیر ۱۶.۵۵ درصد نگه دارد، اما در برابر حمله همچنان آسیب‌پذیر است. این حمله با کمتر از ۱۰ تغییر مشخصه، نرخ موفقیت ۳۶.۳۴ درصد و در شرایط بدون محدودیت پریشیدگی، نرخ موفقیت ۹۴.۵۶ درصد را نشان می‌دهد. یافته‌های این پژوهش بر اهمیت توسعه‌ی تأکید دارند که قادرند با شناسایی نقاط ضعف پنهان در سیستم‌های sigma-binary ابزارهای ارزیابی دقیق نظیر .دفاعی موجود، زمینه‌ساز طراحی سیستم‌های شناسایی بدافزار مستحکم‌تر شوند