تشخیص میزان خطر امنیتی برنامه‌های موبایل با استفاده از مفهوم آنتروپی

محمود دی‌پیر [۱]، تکتم ذوقی [۲]

[۱] دانشیار دانشکده رایانه و فناوری اطلاعات، دانشگاه هوایی شهید ستاری، تهران، ایران
mdeypir@ssau.ac.ir
[۲] استادیار گروه مهندسی کامپیوتر و برق، دانشکده شریعتی، دانشگاه فنی و حرفه‌ای، تهران، ایران
t.zoughi@shariaty.ac.ir

چکیده

امنیت دستگاه‌های همراه با توجه به افزایش کاربرد آنها نقش مهمی در امنیت فضای سایبری دارد. با گسترش کاربرد آنها، بدافزارهای زیادی نیز برای سوء استفاده از کاربران آنها توسط نفوذگران ارائه شده است. شناختن سطح خطر امنیتی هر نرم‌افزار می‌تواند در اطلاع‌رسانی به کاربر درباره استفاده از نرم‌افزارهای مخرب، تأثیرگذار باشد. می‌توان به‌صورت تقریبی خطرات امنیتی نرم‌افزارهای اندروید را از طریق بررسی مجوزهایی که آنها درخواست می‌دهند، تخمین زد. در این بررسی بر اساس تعریف مجوزهای بحرانی و با تجزیه و تحلیل مجوزهای درخواستی توسط نرم‌افزارهای خبیث و نرم‌افزارهای قابل اعتماد و شناخته شده، معیار جدیدی به منظور اندازه‌گیری خطر امنیتی برنامه‌های اندروید ارائه شده است. در این معیار مجوزهایی اثر بیشتری در محاسبه مقدار خطر امنیتی دارند که آنتروپی بیشتری در تشخیص برنامه‌های مخرب از برنامه‌های کاربردی داشته باشند. همچنین میزان خطر هر برنامه موبایل برابر با مجموع بهره اطلاعاتی مجوزهای درخواستی آن است. آزمایش‌های صورت گرفته روی داده‌های واقعی نشان‌دهنده نرخ تشخیص بالاتر معیار پیشنهادی در مقایسه با استانداردهای گذشته قرار دارد.

کلمات کلیدی: مجوز، ارزیابی ریسک امنیتی، معیار امنیتی، داده کاوی، آنتروپی، بهره اطلاعاتی، تحلیل ایستا، تحلیل پویا.

۱ مقدمه

بین تمام سیستم‌های عامل ایجاد شده برای گوشی‌های موبایل و ابزارهای هوشمند قابل حمل، اندروید به‌شکل گسترده‌تری به کار گرفته شده است. برای این پلتفرم، تعداد زیادی برنامه تاکنون توسعه یافته‌اند. اکثریت این برنامه‌ها توسط افراد نامشخص و توسعه‌دهندگان ناشناس عرضه شده‌اند [۲۶-۲۷]. مدل امنیتی برنامه‌ها در سیستم عامل اندروید بر پایه مجوزها استوار است. این مجوزها در ابتدای نصب هر نرم‌افزار یا در زمان اجرای

آن از کاربر پرسیده می‌شوند و غیر از آن، کاربر چندان دخالتی در امنیت نرم افزار مورد استفاده خود ندارد. معمولاً کاربران به‌ندرت زمان کافی را برای مطالعه و توجه به لیست مجوزها در صفحه نصب اولیه نرم‌افزار یا هنگام اجرا تخصیص می‌دهند. علاوه بر این، کاربران عادی معمولاً دانش فنی برای شناخت تأثیر استفاده از هر مجوز و امکان سوء استفاده از آن توسط نفوذگران را ندارند. لذا، این رویکرد امنیتی در افزایش امنیت کاربران به‌منظور حفاظت از داده‌های شخصی و حریم خصوصی آنها کمتر مؤثر است [۲۸-۲۹]. نرم‌افزارهای مخرب، نظیر تروجان‌ها، جاسوس‌افزارها، باج‌افزارها و تبلیغ‌افزارها می‌توانند با فریفتن کاربران، خود را به‌عنوان یک برنامه مفید و بدون خطر ارائه دهند و اطلاعات حساس شرکت‌ها و مراکز حساس دولتی را بدزدند. این نوع بدافزارها همچنین می‌توانند با دزدیدن داده‌های شخصی افراد و فاش کردن آنها، حریم خصوصی آنها را نقض کنند [۳۰-۳۱]. بر اساس آمارهای غیررسمی اخیر، در میان هر ۵ برنامه توسعه‌یافته اندروید، یکی بدافزار بوده است. بنابراین شناسایی و مقابله با این بدافزارها، بسیار ضروری است. تا به حال تحقیقاتی به‌منظور افزایش آگاهی کاربران در زمینه امنیت نرم افزارها در اندروید انجام شده است [۱]. استفاده از عناوین مناسب‌تر برای مجوزها، دسته‌بندی مجوزها، کاهش تعداد عنوان‌های مجوز، بهره‌برداری از نظرات کاربران علاوه بر مجوزها، نمونه‌هایی از راه‌کارهای ارائه شده در این تحقیقات هستند. همچنین، تاکنون معیارهای مختلفی نیز برای سنجش خطر امنیتی یک نرم‌افزار اندرویدی ارائه شده است. تعداد مجوزهای حساس درخواستی و تعداد جفت مجوزهای حساس درخواستی نمونه‌هایی از این معیارها هستند [۲]. با بهره‌گیری از این استانداردها و وجود یک حد مرجع، پس از ارزیابی ریسک امنیتی یک برنامه مظنون، اگر ریسک آن افزایش یافته باشد، اخطاری به لحاظ امنیتی منتشر می‌شود. در این نوشتار، یک استاندارد نوآورانه برای ارزیابی ریسک یک برنامه اندرویدی مطرح شده که نسبت به استانداردهای پیشین کارکرد بهینه‌تری دارد.

در ادامه، تعدادی از پژوهش‌های انجام شده که با امنیت اندروید ارتباط دارند، معرفی می‌شوند. در بخش سوم، استاندارد تازه پیشنهادی ارائه و روش محاسبه آن توضیح داده شده است. در قسمت چهارم، تجربیاتی به‌منظور ارزیابی و تطبیق استاندارد پیشنهادی با استانداردهای پیشین، عرضه شده‌اند. در این بخش، با بهره‌گیری از دسته داده‌هایی شامل صدها بدافزار و هزاران برنامه مفید شناخته شده اندروید، معیار پیشنهادی با معیار ارائه شده قبلی از نظر اندازه‌گیری میزان خطر و توان تشخیص بدافزارها از نرم‌افزارها مقایسه خواهد شد. در نهایت این مقاله در بخش پنجم جمع‌بندی و نتیجه‌گیری می‌شود.

۲ مروری بر کارهای دیگران

با نگاه به ساختار امنیتی خصوصی اندروید و محدودیت‌های آن، تعدادی تحقیق در این زمینه صورت گرفته است. مطالعات اشاره دارند که کاربران اکثراً از بررسی مجوزهای پیشنهادی برنامه‌ها در اندروید چشم‌پوشی می‌کنند. در برخی تحقیقات انجام‌شده، سعی شده تا بر این مشکل غلبه شود [۳-۶]. فلت و همکاران [۳] راهکارهایی نظیر تغییر طبقه‌بندی مجوزها، تأکید بر مفهوم ریسک امنیتی و روش تخصیص مجوزها مطرح کرده‌اند. در [۷] اطلاعات سطح بالا شامل عناصر حفظ حریم شخصی همچون اطلاعات شخصی، مکان و دفترچه تلفن، به‌جای لیست مجوزها در صفحه توصیف برنامه پیشنهاد شده است. به‌منظور کاهش فضای

لازم برای نمایش چنین اطلاعاتی و کمک به کاربر در تصمیم‌گیری بهینه‌تر هنگام انتخاب و نصب، در [۱] عوامل ریسک و غیر ریسک که نتایج کمی آنها با توجه به مجوزها قابل محاسبه است، ارائه گردیده‌اند. با بررسی کاربران معلوم شد که این استانداردها نسبت به اطلاعات متنی تأثیر بیشتری دارند. پنگ و همکاران [۸] یک روش اصلی بر اساس مدل احتمالاتی را به‌منظور رتبه‌بندی برنامه‌های اندروید بر پایه مجوزهای مورد نیاز، عرضه کردند. برخی از تحقیقات با استفاده از مجوزهای پیشنهادی برنامه‌ها، به تشخیص برنامه‌های زیان‌آور یا مشکوک می‌پردازند [۹-۱۱]. برخی دیگر نیز با استفاده از تحلیل استاتیکی کد برنامه، توابع استفاده شده در برنامه‌نویسی و هم‌خوانی آن با برخی الگوهای موجود بدافزارها، برای تشخیص بدافزارهای جدید اقدام کرده‌اند [۱۲-۱۵]. تعدادی از پژوهشگران ترکیبی از تحلیل ایستا و پویا را به‌منظور تخمین خطر امنیتی نرم‌افزارهای اندروید مورد توجه قرار داده‌اند [۲۱]. اخیراً یادگیری عمیق به‌صورت گسترده به‌منظور تشخیص بدافزارهای اندروید مورد توجه قرار گرفته است [۲۲-۲۴]. در این دسته از تحقیقات عمدتاً محتوای برنامه‌های اندروید اعم از نرم‌افزار و بدافزار مانند تصاویر دو بعدی فرض می‌شوند و از آنها، ویژگی‌هایی به‌منظور آموزش یک مدل عمیق دسته‌بندی استفاده می‌گردد [۳۲-۳۳].

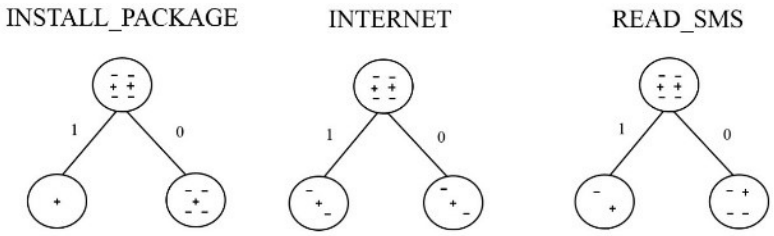
۳ روش پیشنهادی

یک مجوز بحرانی، مجوزی است که پیشتر در نرم‌افزارهای زیان‌آور اندروید مورد شناسایی و استفاده قرار گرفته است، یا به منابع حساس نرم‌افزاری و سخت‌افزاری دستگاه دسترسی پیدا می‌کند. از این استانداردها می‌توان برای ارائه هشدار در مورد اپلیکیشن‌های مظنون یا تشخیص نرم‌افزارهای زیان‌آور ناشناس جدید، بهره برد. ما در جستجوی یک استاندارد، برای ارزیابی ریسک‌های امنیتی نرم‌افزارهای اندروید هستیم که هم ساده باشد و هم توصیف دقیق‌تری از ریسک امنیتی اپلیکیشن در اندروید ارائه دهد. علاوه بر این، توانایی داشته باشد تا به نرم‌افزارهای سودمند، میزان ریسک امنیتی کم و به نرم‌افزارهای زیان‌آور، نسبت به نرم‌افزارهای سودمند، میزان ریسک امنیتی بالایی اختصاص دهد. استاندارد پیشنهادی ما بر مبنای نظریه اطلاعات و اصول آنتروپی که در یادگیری ماشین به‌کار برده شده است، ارائه شده است. در این استاندارد، بهره‌گیری اطلاعاتی از مجوزها محاسبه می‌شود. این بهره‌گیری اطلاعاتی با توجه به مفهوم آنتروپی قابل محاسبه است. در حقیقت، ما با توجه به اصول حوزه نظریه اطلاعات، آنتروپی مجموعه کل اپلیکیشن‌ها از لحاظ مفید و زیان‌آور بودن را محاسبه می‌کنیم و سپس با توجه به نقش هر مجوز در تفکیک اولیه نرم‌افزارها از بدافزارها، بهره‌گیری اطلاعاتی را برای هر مجوز به دست می‌آوریم. از دیدگاه ما، یک مجوز حیاتی است که بهره‌گیری اطلاعاتی بالایی در تفکیک نرم‌افزارها از بدافزارهای دارد. مجموع بهره اطلاعاتی که مجوزهای مورد استفاده یک اپلیکیشن اندروید دارند، میزان ریسک امنیتی آن را پیش‌بینی می‌کند. ما روش کار را با استفاده از مثال زیر نشان می‌دهیم.

مثال: فرض کنید مجموعه شش نرم‌افزار مفید و مخرب (بدافزار) مورد تحلیل ما به صورت جدول ۱ باشد. در این چارت، برای هر اپلیکیشن اندروید، شناسه، فهرست مجوزهای آن، و همچنین ویژگی مفید یا زیان‌آور

جدول ۱: اطلاعات وابسته به مثال ۱: اپلیکیشن‌های سودمند (−) و برنامه‌های مخرب (+)

ID	Permissions	Malware
1	INTERNET, READ_PROFILE	-
2	BATTERY_STATS, BLUETOOTH	-
3	BROADCAST_SMS,WRITE_SMS	+
4	INTERNET,INSTALL_PACKAGE, READ_SMS	+
5	READ_SMS, WRITE_EXTERNAL_STORAGE	-
6	BATERY_STATS, INTERNET	-



شکل ۱: تأثیر بهره‌گیری از سه مجوز نمونه در تفکیک برنامه‌های بدخواه (+) از اپلیکیشن‌ها (−)

بودن آن مشخص شده است.

باید برای هر مجوز، بهره اطلاعاتی را با استناد به داده‌های جدول فوق محاسبه نماییم و از این داده‌ها و معیار ارائه شده، به‌منظور ارزیابی ریسک امنیتی اپلیکیشن‌های اندروید بهره ببریم. مسلماً هر مجوز، با توجه به اطلاعات ارائه شده در جدول ذکر شده، بهره‌ای متفاوت از اطلاعات خواهد داشت و با توجه به این بهره‌گیری اطلاعاتی، در تعیین ریسک امنیتی یک برنامه تازه تاثیرگذار خواهد بود. به‌عنوان نمونه، بهره اطلاعاتی را برای سه مجوز نمونه با استفاده از شکل ۱ محاسبه کرده‌ایم. در این شکل، نماد مثبت نشان‌دهنده‌ی برنامه‌های مخرب و نماد منفی، نمایانگر تست منفی یا به‌عبارتی اپلیکیشن‌های مفید است.

همان‌گونه که در شکل ۱ آشکار است، برای هر مجوز، بر اساس استفاده (داشتن مقدار ۱) و عدم استفاده (مقدار ۰)، برنامه‌ها به دو گروه تقسیم شده و یک درخت شامل یک ریشه و دو زیرشاخه تشکیل می‌شود. زیرشاخه سمت چپ نمایانگر گروهی از برنامه‌هاست که این مجوز را خواستار شده‌اند و زیرشاخه سمت راست برنامه‌هایی را نشان می‌دهد که نیازی به این مجوز برای اجرای خود ندارند. در هر گروه، ممکن است هم برنامه‌های بدخواه و هم اپلیکیشن‌های مفید وجود داشته باشد. میزان آنتروپی مجموعه اپلیکیشن‌ها، با دسته‌بندی انجام شده توسط هر مجوز، می‌تواند کاهش یابد و در نتیجه بهره‌گیری اطلاعاتی بیشتر از صفر به‌دست آید. به‌عنوان مثال، بهره اطلاعاتی را برای مجوز INSTALL_PACKAGE محاسبه می‌کنیم. از آنجا که مجموعه اپلیکیشن‌های تحت تجزیه و تحلیل در اینجا ۶ است و از این تعداد ۲ نمونه برنامه‌های بدخواه

هستند، آنتروپی ریشه درخت یعنی مجموعه کل اپلیکیشن‌ها مساوی خواهد بود با:

$$\text{ParentEntropy} = -\frac{۲}{۶}\log_۲\left(\frac{۲}{۶}\right) - \frac{۴}{۶}\log_۲\left(\frac{۶}{۶}\right) = ۰/۷۹۸۶ \quad (۱)$$

بر اساس مجموعه اپلیکیشن‌های نمونه ما در جدول ۱، فقط یک نوع نرم‌افزار مخرب از این مجوز استفاده نموده است. یک نرم‌افزار مخرب و چهار اپلیکیشن مفید از این مجوز بهره نبرده‌اند. در نتیجه، آنتروپی این فرزندان به‌شکل متوالی برابر خواهد بود با:

$$\text{Entropy}(\text{INSTALL\_PACKAGES} = ۱) = -\frac{۱}{۱}\log_۲\left(\frac{۱}{۱}\right) = ۰ \quad (۲)$$

$$\text{Entropy}(\text{INSTALL\_PACKAGES} = ۰) = -\frac{۱}{۵}\log_۲\left(\frac{۱}{۵}\right) - \frac{۴}{۵}\log_۲\left(\frac{۴}{۵}\right) = ۰/۶۴۲۹ \quad (۳)$$

میانگین وزنی آنتروپی گره‌های فرزند با توجه به تعداد هر کدام به‌صورت زیر محاسبه می‌شود:

$$\text{WeightedAverageEntropyofChildren} = \frac{۱}{۶} \times ۰ + \frac{۵}{۶} \times ۰/۶۴۲۹ = ۰/۵۳۵۸ \quad (۴)$$

با توجه به آنتروپی‌های محاسبه شده، میزان بهره اطلاعاتی برای این مجوز، معادل با تفاوت بین آنتروپی کل نرم‌افزارها و میانگین وزن‌دار آنتروپی زیردرخت‌ها می‌باشد:

$$\text{IG}(\text{INSTALL\_PACKAGES}) = ۰/۷۹۸۶ - ۰/۵۳۵۸ = ۰/۲۶۲۸ \quad (۵)$$

در معیار ارائه شده توسط ما، این رقم، میزان ریسک امنیتی مربوط به این مجوز را ارائه می‌دهد. مقدار بهره اطلاعاتی یا سطح خطر امنیتی دو مجوز INTERNET و READ_SMS به‌شکل زیر تعیین می‌شود، که ما از جزئیات محاسباتی صرف نظر می‌کنیم و این محاسبات را به عهده مطالعه‌گر می‌گذاریم:

$$\text{IG}(\text{INTERNET}) = ۰ \quad (۶)$$

$$\text{IG}(\text{READ\_SMS}) = ۰/۰۳۹۲ \quad (۷)$$

با توجه به اعداد می‌توان گفت که در استفاده از مجوز INTERNET هیچ تفاوتی بین بدافزار و نرم‌افزارها نیست. اگرچه مجوز READ_SMS یک بهره اطلاعاتی کمتر نسبت به INSTALL_PACKAGES دارد، اما باعث تمایز بدافزارها از نرم‌افزارهای عادی می‌شود و به زبان دقیق‌تر، خطر امنیتی کمتری را داراست. باید به این نکته توجه داشت که خطر امنیتی برای تمامی مجوزهای اندروید بر اساس نرم‌افزارها و بدافزارهای شناسایی شده محاسبه می‌شود. ما این فرایند را برای تمامی مجوزها انجام داده‌ایم. هرچند که ایده ما از

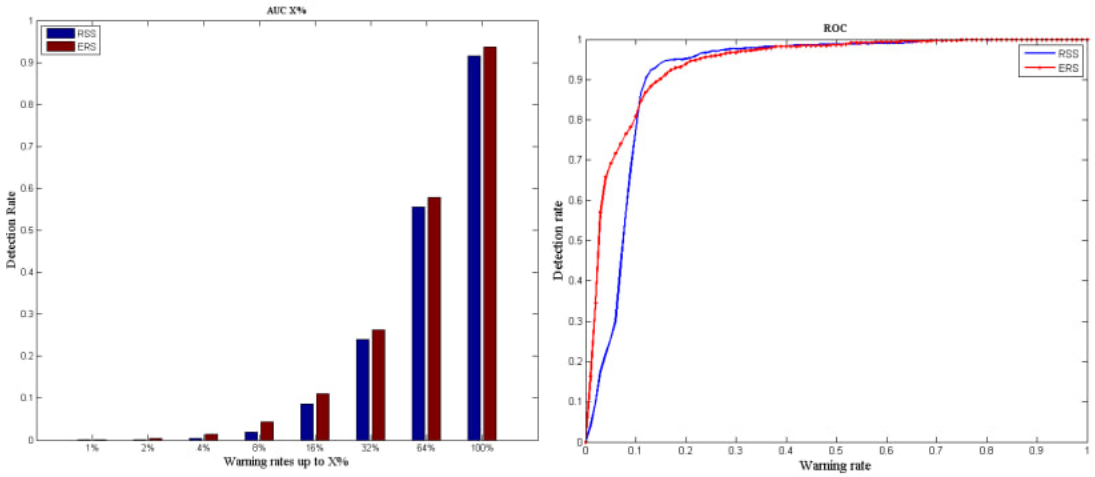
یادگیری ماشین و ساخت درخت تصمیم براساس بهره اطلاعاتی مشتق شده است، اما معیار ما یک هدف کاملاً متفاوت دارد. نخست، هدف ما در این‌جا دسته‌بندی نیست، بلکه محاسبه یک مقدار عددی برای خطر امنیتی برنامه بر اساس آنتروپی و بهره اطلاعاتی مجوزها می‌باشد و ما در این‌جا داده‌ها را لیبل نمی‌زنیم. دوم، ما بهره اطلاعاتی را به‌صورت جداگانه برای همه مجوزها محاسبه می‌کنیم، در حالی که در یک مدل دسته‌بندی، از یک ویژگی شروع به ساخت یک درخت تصمیم کرده و در سطوح مختلفی ساخته می‌شود. فرض کنید با توجه به محاسبات انجام شده، یک برنامه اندرویدی با نام A داریم که از تمامی سه مجوز فوق استفاده کرده است. میزان خطر امنیتی این برنامه به شرح زیر می‌باشد:

$$\text{Risk(A)} = ۰٫۲۶۲۸ + ۰٫۰۳۹۲ + ۰ = ۰٫۳۰۲۰ \quad (۸)$$

این عدد با احتمال مخرب بودن نرم‌افزارِ در دست بررسی، متناسب است. به این معنا که هر چقدر مقدار خطر امنیتی بیشتر باشد، احتمال آسیب‌پذیری برنامه نیز بالاتر است. البته، داشتن یک ریسک امنیتی برای یک برنامه حتماً به معنی آلوده بودن آن به بدافزار نیست، بلکه یک هشدار برای کاربران می‌باشد و یا می‌تواند به عنوان یک پردازش پیشین برای تجزیه و تحلیل‌های دقیق‌تر به‌منظور شناسایی دقیق تهدیدات به کار برده شود. علاوه بر این، میزان خطر امنیتی نسبی است و می‌تواند به انتخاب یک برنامه بهتر و کم‌ریسک‌تر کمک کند. به این ترتیب که با وجود چندین برنامه با قابلیت‌های مشابه و ریسک‌های امنیتی متفاوت، منطقی است که برنامه‌ای با خطر امنیتی کمتر انتخاب شود.

۴ ارزیابی

به‌منظور ارزیابی، با استفاده از مجموعه داده‌های متنوع، روش پیشنهادی با معیارهای مختلف مقایسه شده است. معیارها در نرم‌افزار متلب پیاده‌سازی شده و مورد ارزیابی قرار گرفته‌اند. با توجه به محدودیت صفحات مقاله، تنها نتایج به‌دست آمده از یک مورد از آزمایش‌ها در اینجا گزارش می‌شود. در اینجا، یک مجموعه داده بدافزار و یک مجموعه داده نرم‌افزار برای مقایسه استفاده می‌شوند. مجموعه داده بدافزار شامل ۲۱۲۸ برنامه مفید است که از پلتفرم‌های داخلی فروش برنامه، دانلود و استخراج مجوز شده‌اند. مجموعه داده بدافزار شامل ۱۰۱۴ برنامه اندروید مخرب است است که از منابع مختلف گردآوری و استخراج مجوز شده‌اند. با استفاده از این دو مجموعه داده روش پیشنهادی مبتنی بر آنتروپی ERS (Entropy Based Risk) با روش RSS (Rarity Based Risk Score) که در مرجع [۳] ارائه شده، از نظر نرخ تشخیص بدافزار، مقایسه شده است. در این تجربه، تمرکز بر روی قابلیت شناسایی این معیارها است. یعنی یک معیار موفق است که بتواند به‌طور متناسب برای تهدیدات مقدار خطر امنیتی بیشتری ارزیابی کند. به‌عبارتی، اگر ما برای همه برنامه‌های کاربردی و تهدیدات مقدار ریسک را بر اساس یک معیار محاسبه کنیم و سپس فهرست کلی برنامه‌ها را به‌صورت نزولی بر اساس مقدار ریسک مرتب کنیم، برنامه‌های مخرب بیشتری نسبت به برنامه‌های مفید در بالای فهرست قرار خواهند گرفت. به این منظور، ما در این آزمایش مجموعه‌ای از برنامه‌های مفید و



(الف) نمودار ROC (ب) سطح زیر نمودار (AUC)

شکل ۲: مقایسه نرخ تشخیص معیار پیشنهادی ERS با معیار قبلی RSS بر حسب سطح هشدار

مجموعه‌ای از برنامه‌های مخرب را در یک فهرست یکپارچه قرار داده و با استفاده از ۹۰ درصد فهرست حاصل مدل خود را به وجود آورده‌ایم. سپس با استفاده از ۱۰ درصد باقی‌مانده، به آزمون روش خود می‌پردازیم. به این صورت که با استفاده از مدل تهیه شده، خطر امنیتی آنها را محاسبه کرده و سپس به صورت نزولی مرتب کرده‌ایم. حالا، در هر دوره، درصدهای مختلفی از برنامه‌های برتر فهرست مربوطه را انتخاب کرده و بررسی می‌کنیم که چه نسبتی از تهدیدات در این بخش از فهرست قرار دارند. به درصدهای انتخاب شده از فهرست، سطح هشدار و به درصدهای شناسایی شده تهدیدات، نرخ شناسایی می‌گویند. واضح است که هرچه معیار قدرتمندتر باشد، درصد بیشتری از تهدیدات در بالای فهرست قرار خواهند گرفت و نرخ شناسایی بالاتری خواهد داشت. شکل ۲، بخش‌های الف و ب، به ترتیب منحنی‌های ROC به دست آمده، و سطح زیر نمودار AUC را برای معیار پیشنهادی ERS و معیار RSS [۳] نمایش می‌دهند. در این شکل، محورهای افقی و عمودی به ترتیب نرخ هشدار (Warning Rate) و نرخ شناسایی (Detection Rate) می‌باشند.

همان‌طور که در بخش (الف) شکل ۲ دیده می‌شود، برای مقادیر کم سطح هشدار، روش پیشنهادی ERS از RSS بهتر عمل می‌کند. اما با افزایش سطح هشدار، RSS بهتر عمل کرده است. در بخش (ب) شکل ۲ مشاهده می شود که سطح کلی زیر نمودار به‌ازای مقادیر مختلف نرخ هشدار بیشتر است، زیرا روش پیشنهادی در سطوح هشدار کمتر، برتری قابل توجه‌تری به‌دست آورده است. علت برتری روش پیشنهادی را می‌توان در استفاده از آنتروپی برای متمایز کردن بدافزارها از نرم‌افزارهای مفید، جستجو کرد.

۵ جمع‌بندی و نتیجه‌گیری

معمولاً، برنامه‌های مخرب در سیستم عامل اندروید تلاش می‌کنند تا خود را به عنوان یک اپلیکیشن مفید جلوه دهند. در این زمینه، آنها باید از تعدادی مجوز برای انجام وظایف مفیدشان استفاده کنند، همچنین، برای

اجرای عملیات‌های زیان‌آور نیز به برخی دیگر از مجوزها نیاز دارند. این مسئله باعث می‌شود که کل الگوی استفاده‌شان از مجوزها با اپلیکیشن های مفید متفاوت باشد و در نتیجه، خطر امنیتی ایجاد شده توسط آنها افزایش یابد. ولی ممکن است برخی نرم‌افزارها وجود داشته باشند که مجوزهایی که از آنها استفاده می‌کنند، به‌شدت به بدافزارها شبیه باشد. در این وضعیت، حتی با استفاده از یک معیار امنیتی، برای آنها نیز یک خطر امنیتی بالا تخمین زده می‌شود و معیار پیشنهادی نیز از این قانون استثنا نیست، هرچند که نسبت به سایر معیارها کارآیی بهتری دارد. برای شناسایی دقیق‌تر بدافزارها، استفاده از روش‌های تکمیلی نظیر تجزیه و تحلیل کدهای ایستا و پویا و همچنین تکنیک‌های داده‌کاوی ضروری است. معیار پیشنهادی ما که از ایده‌های آنتروپی و بهره اطلاعات مجوزها برای تشخیص مجوزهای حساس استفاده می‌کند، به نظر می‌رسد که نسبت به معیارهای پیشنهادی پیشین به‌شکل بهتری عمل کند. آزمایش‌ها بر روی مجموعه داده‌های واقعی نشان داده‌اند که معیار پیشنهادی، نسبت به نرم‌افزارهای مفید، مقدار خطر قابل توجه‌تری را ارائه می‌دهد.

مراجع

[1] C. Wilson, “Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress”, Washington, DC, 2008.

[2] C. S. Gates, J. Chen, N. Li, and R. W. Proctor, “Effective risk communication for android apps”, Dependable and Secure Computing, IEEE Transactions on, 11(3), 2014, pp. 252-265.

[3] C. S. Gates, N. Li, H. Peng, B. Sarma, Y. Qi, R. Potharaju, and I. Molloy, “Generating summary risk scores for mobile applications”, Dependable and Secure Computing, IEEE Transactions on, 11(3), 2014, pp. 238-251.

[4] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, “Measuring user confidence in smartphone security and privacy”, In Proceedings of the Eighth Symposium on Usable Privacy and Security, ACM, July 2012. P.1.

[5] [5] A. P. Felt, K. Greenwood, and D. Wagner, “The effectiveness of application permissions,” In Proceedings of the 2nd USENIX conference on Web application development, June 2011, p.7.

[6] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, “Android permissions: User attention, comprehension, and behavior”, Tech. Rep. UCB/EECS-2012-26, UC Berkeley, 2012.

[7] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, “A conundrum of permissions: installing applications on an android smartphone”, In Financial Cryptography and Data Security, Springer Berlin Heidelberg, 2012, pp. 68-79.

[8] P. G. Kelley, L. F. Cranor, and N. Sadeh, “Privacy as part of the app decision-making process”, In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, April 2013, pp. 3393-3402.

[9] H. Peng, C. Gates, B. Sarma, N. Li, Y. Qi, R. Potharaju, R., and I. Molloy, "Using probabilistic generative models for ranking risks of android apps", In Proceedings of the 2012 ACM conference on Computer and communications security, ACM, October 2012, pp. 241-252.

[10] D. Geneiatakis, I. N. Fovino, I. Kounelis, and P. Stirparo, "A Permission verification approach for android mobile applications", Computers & Security, 49, 2015, pp.192-205.

[11] B. P. Sarma, N. Li, C. Gates, R. Potharaju, C. Nita-Rotaru, and I. Molloy, "Android permissions: a perspective combining risks and benefits", In Proceedings of the 17th ACM symposium on Access Control Models and Technologies, June 2012, pp. 13-22.

[12] L. Cen, C. Gates, L.Si, and N. Li, "A probabilistic discriminative model for android malware detection with decompiled source code", In Dependable and Secure Computing, IEEE Transactions on, vol.12, no.4, 2015, pp.400-412.

[13] A. Desnos, "Android: Static analysis using similarity distance", In System Science (HICSS), 2012 45th Hawaii International Conference on, January 2012, pp. 5394-5403.

[14] A. D. Schmidt, R. Bye, H. G. Schmidt, J. Clausen, O. Kiraz, K. Yüksel, and S. Albayrak, "Static analysis of executables for collaborative malware detection on android", In Communications, 2009. ICC'09. IEEE International Conference on, June 2009, pp. 1-5.

[15] Y. Zhou, Z. Wang, W. Zhou, and X. Jiang, "Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets", In NDSS, Vol. 25, No. 4, February 2012, pp. 50-52.

[16] Y. Aafer, W. Du, and H. Yin, "DroidAPIMiner: Mining API-level features for robust malware detection in android", In Security and Privacy in Communication Networks, 2013, pp. 86-103.

[17] M. Christodorescu, S. Jha, C. Kruegel, "Mining specifications of malicious behavior", In Proceedings of the 1st India software engineering conference, ACM, February 2008, pp. 5-14.

[18] K. Rieck, T. Holz, C. Willems, P. Düssel, and P. Laskov, "Learning and classification of malware behavior", In Detection of Intrusions and Malware, and Vulnerability Assessment, 2008, pp. 108-125.

[19] A. Shabtai, and Y. Elovici, "Applying behavioral detection on android-based devices", In Mobile Wireless Middleware, Operating Systems, and Applications, 2010, pp. 235-249.

[20] I. Burguera, U. Zurutuza, and S. Nadjm-Tehrani, "Crowdroid: behavior-based malware detection system for android", In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, October 2011, pp. 15-26.

[21] H. X. Son, B. Carminati, and E. Ferrari, "A Risk Estimation Mechanism for Android Apps based on Hybrid Analysis", Data Science and Engineering, 2022, pp.1-11.

[22] K. Bakour, and H.M. Ünver, "DeepVisDroid: android malware detection by hybridizing image-based features with deep learning techniques", Neural Computing and Applications, 33, 2021, pp. 11499-11516.

[23] J. Geremias, E. K. Viegas, A. O. Santin, A. O., A. Britto, and P. Horchulhack, "Towards multi-view android malware detection through image-based deep learning", In 2022 International Wireless Communications and Mobile Computing (IWCMC), 2022, pp. 572-577.

[24] I. Almomani, A. Alkhayer, and W. El-Shafai, "An automated vision-based deep learning model for efficient detection of android malware attacks", IEEE Access, 10, 2022, pp. 2700-2720.

[25] R. Quinlan, "Learning efficient classification procedures", Machine Learning: an artificial intelligence approach, Michalski, Carbonell & Mitchell (eds.), Morgan Kaufmann, 1983, pp. 463-482.

[26] Ali, Atif, Nafees Ahmed Somroo, Umer Farooq, Muhammad Asif, Iman Akour, and Wathiq Mansoor. "Smartphone Security Hardening: Threats to Organizational Security and Risk Mitigation". In 2022 International Conference on Cyber Resilience (ICCR), 2022, pp. 1-12. IEEE.

[27] Lin, Wenjun, Ming Xu, Jingyi He, and Wenjun Zhang. "Privacy, security and resilience in mobile healthcare applications". Enterprise Information Systems 17, no. 3, pp.1939896, 2023.

[28] Gull, Hina, Saqib Saeed, Sardar Zafar Iqbal, Yasser A. Bamarouf, Mohammed A. Alqahtani, Dina A. Alabbad, Madeeha Saqib, Saeed Hussein Al Qahtani, and Albandary Alamer. "An empirical study of mobile commerce and customers security perception in Saudi Arabia". Electronics 11, no. 3, pp 293, 2022.

[29] Cinar, Ahmet Cevahir, and Turkan Beyza Kara. "The current state and future of mobile security in the light of the recent mobile security threat reports". Multimedia Tools and Applications. pp. 1-13, 2023.

[30] Kambar, Mina Esmail Zadeh Nojoo, Armin Esmaeilzadeh, Yoohwan Kim, and Kazem Taghva. "A survey on mobile malware detection methods using machine learning". In 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0215-0221, 2022.

[31] Kim, Yu-kyung, Jemin Justin Lee, Myong-Hyun Go, Hae Young Kang, and Kyungho Lee. "A systematic overview of the machine learning methods for mobile malware detection". Security and Communication Networks, 2022.

[32] Sk, Heena Kauser. "A literature review on android mobile malware detection using machine learning techniques". In 2022 6th international conference on computing methodologies and communication (ICCMC), pp. 986-991, 2022.

[33] Ullah, Farhan, Xiaochun Cheng, Leonardo Mostarda, and Sohail Jabbar. "Android-IoT Malware Classification and Detection Approach Using Deep URL Features Analysis." Journal of Database Management (JDM), 2023, vol. 34, no. 2, pp. 1-26.