گزارشِ تحقیق درباره‌ی دسترسیِ اپلیکیشن‌ها در سیستم‌عامل اندروید

تهیه و تنظیم: مبین خیبری

شماره دانشجویی: 994421017

استاد راهنما: دکتر میرسامان تاجبخش

چکیده:

در گزارشِ پیش‌رو قصد داریم درباره‌ی سطوحِ مختلفِ دسترسی‌های تعریف‌شده برای انواع برنامه‌های اندرویدی، به‌خصوص پلتفرم‌اپلیکیشن‌ها و نیز برنامه‌های سیستمی پژوهش کنیم. این نوع اپلیکیشن‌ها عموما Platform Signature Apps نامیده می‌شوند و به طور پیش‌فرض روی برخی تلفن‌های همراه نصب شده‌اند.

هر آنچه باید درباره دسترسی های اندروید بدانیم:

دسترسی اپلیکیشن‌ها به سایر برنامه‌های دستگاه می‌تواند راهی برای نفوذ به اطلاعات شخصی کاربر توسط افراد سودجو باشد. با انجام تنظیماتی که در این گزارش ذکر می‌کنیم، می‌توانید دسترسی‌های غیرضروری اپلیکیشن‌ها را غیرفعال کنید.

اپلیکیشن‌ها درکنار اجزایی مانند نمایشگر، پردازنده، حافظه‌ی رم، باتری و دوربین، نقش مهمی در گوشی‌ها و تبلت‌های هوشمند دارند و این دستگاه‌ها را کاربردی کرده‌اند. اپلیکیشن‌ها به ارتقای تجربه‌ی کاربری دستگاه‌های امروزی کمک کرده‌اند و با استفاده از آن‌ها انجام کارهای زیادی مانند دسترسی به پلتفرم‌های شبکه‌ی اجتماعی، مشاهده‌ی وضعیت آب‌وهوا و برقراری تماس‌های صوتی و تصویری امکان‌پذیر شده است.

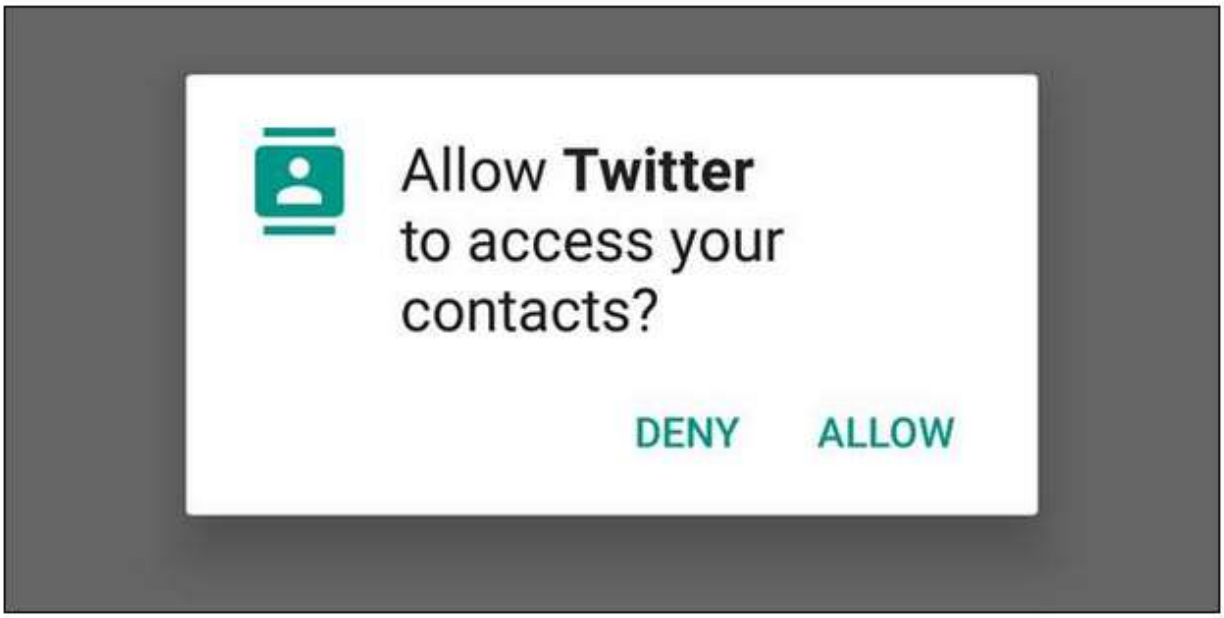
نصب و دانلود اپلیکیشن‌ها کار ساده‌ای است؛ اما باید امنیت اطلاعاتمان را نیز درنظر داشته باشیم. برنامه‌های مخرب پس از نصب می‌توانند به اطلاعات دستگاه کاربر دسترسی داشته باشند؛ به همین دلیل، دسترسی‌های مجاز اپلیکیشن (app permissions)برای محافظت از اطلاعات کاربران ایجاد شده است. مدیریت دسترسی‌ها در نسخه‌های جدیدتر اندروید ارتقا یافته است و کاربران اندرویدی از زمان عرضه‌ی اندروید ۶ مارشمالو می‌توانند دسترسی‌های اپلیکیشن را کنترل و گزینه‌های دسترسی را انتخاب کنند.

در این گزارش، پس از مرور کاربرد دسترسی‌ها، غیرفعال‌کردن گزینه‌های غیرضروری را برای امنیت بیشتر و حفاظت از اطلاعات آموزش می‌دهیم.

دسترسی‌های اپلیکیشن چیست؟

معمولا پیش از نصب اپلیکیشن، فهرستی از برنامه‌هایی به کاربر نشان داده می‌شود که آن اپلیکیشن می‌تواند به آن‌ها دسترسی داشته باشد. ویژگی دسترسی‌های اپلیکیشن، همان‌طور که از نامش مشخص است، به اپلیکیشن‌ها امکان دسترسی به برنامه‌های دیگر دستگاه از اطلاعات ذخیره‌شده، فهرست مخاطبان و فایل‌های رسانه گرفته تا سخت‌افزارهایی مانند دوربین و میکروفون را می‌دهد .درواقع، اپلیکیشن‌ها برای عملکرد بهتر به برخی از دسترسی‌ها نیاز دارند و دسترسی‌ها اجازه‌ی سیستم به اپلیکیشن برای دسترسی به اپلیکیشن‌های دیگر است.

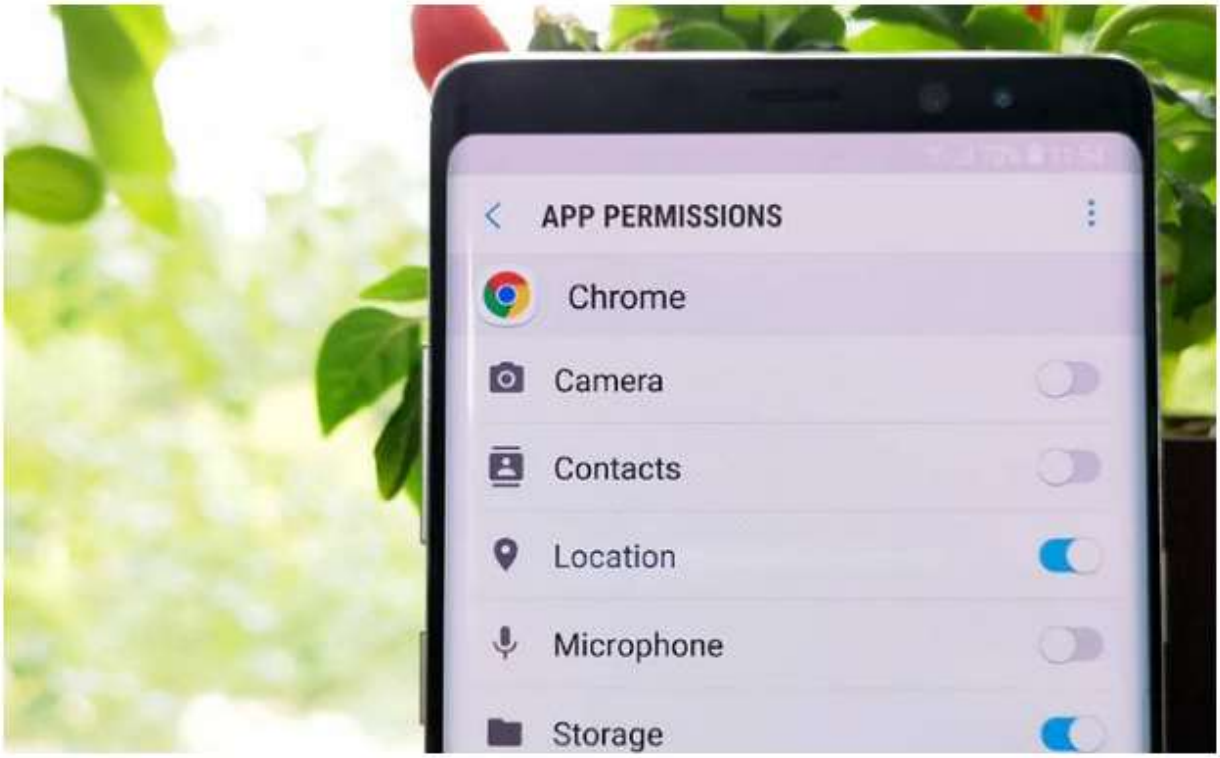
اپلیکیشن‌ها به‌طور خودکار مجاز به دسترسی به برنامه‌های دیگر نیستند و برای این کار به تأیید کاربر نیاز دارند. پس با لغو دسترسی، اپلیکیشن نمی‌تواند از برنامه‌های دیگر استفاده کند. اپلیکیشن‌های قدیمی‌تر پس از غیرفعال‌کردن برخی دسترسی‌های مجاز، به خوبی اجرا نمی‌شوند؛ اما این مشکل برای اپلیکیشن‌های جدید برطرف شده و کاربر می‌تواند به انتخاب خودش دسترسی به برخی قابلیت‌ها را غیرفعال کند؛ البته امکان فعال‌کردن آن‌ها در زمان دیگر وجود دارد و اپلیکیشن در زمان اجرای برخی قابلیت‌ها، برای فعال‌کردن دسترسی‌های لازم به کاربر پیام می‌دهد.



دسترسی‌های عادی و خطرناک

دسترسی به سیستم‌ها می‌توانند عادی یا خطرناک باشد. دسترسی‌های عادی به‌طور پیش‌فرض فعال می‌شوند و حریم خصوصی کاربر را تهدید نمی‌کنند. از دسترسی‌های عادی می‌توان دسترسی خودکار اپلیکیشن‌ها به اینترنت را مثال زد که بدون اجازه‌ی کاربر این ارتباط برقرار می‌شود. برای دسترسی‌های خطرناک نیز می‌توان به دسترسی به تاریخچه‌ی تماس، پیام‌های خصوصی، مکان، دوربین و میکروفون در برخی اپلیکیشن‌ها اشاره کرد.

به‌طور کلی، تجربه‌ی کاربریِ دسترسی‌ها در نسخه‌های جدیدتر اندروید بهبود یافته و گوگل حریم خصوصی و امنیت کاربر را ارتقا بخشیده است .می‌توانید پیش از نصب اپلیکیشن، فهرست دسترسی‌ها را تأیید کنید و درصورت غیرمرتبط‌بودن موارد، برنامه را نصب نکنید. در اندروید ۱۰، گزینه‌ای وجود دارد که فقط درصورت استفاده از برنامه، دسترسی به مکان فعال می‌شود .بنابراین، برنامه‌هایی مانند گوگل مپس، همیشه نمی‌توانند کاربر را ردیابی کنند و فقط درصورت استفاده از برنامه، این دسترسی فعال می‌شود. در این نسخه‌ی اندروید، قابلیت جدید با وجود مفیدبودنش فقط به دسترسی به مکان محدود شده است. در اندروید ۱۱ این ویژگی ارتقا یافته و علاوه‌بر مکان می‌توان دسترسی به دوربین و میکروفون را به زمان استفاده از اپلیکیشن محدود کرد.



هر اپلیکیشن عملکرد خاصی دارد و گاهی در فهرست دسترسی‌های مجاز گزینه‌هایی می‌بینیم که به عملکرد آن اپلیکیشن ربطی ندارند. در ادامه، دسترسی‌های اصلی در دستگاه آورده شده است که درصورت تأیید هرکدام، اپلیکیشن به توضیحات داده‌شده دسترسی پیدا می‌کند.

- حسگرهای بدن: اطلاعات سلامت مانند پایش ضربان قلب
- تقویم: خواندن، ایجاد و ویرایش و حذف رویدادهای تقویم دستگاه
- دوربین: عکس‌برداری و ضبط ویدئو
- مخاطبان: خواندن، ویرایش و ایجاد فهرست مخاطبان و دسترسی به حساب‌های استفاده‌شده در دستگاه

- مکان: دسترسی به موقعیت مکانی مخاطب با استفاده ازGPS ، وای‌فای یا اتصال داده
- میکروفون: ضبط صدا ازجمله در فیلم‌برداری
- موبایل :دسترسی به شماره موبایل و اطلاعات شبکه‌ی گوشی کاربر برای تماس تلفنی، VoiceMailو فورواردکردن تماس و ویرایش تاریخچه‌ی تماس
- :SMSخواندن، دریافت و ارسال پیامک وMMS
- حافظه‌ی ذخیره‌سازی: خواندن و نوشتن فایل‌ها در حافظه‌ی ذخیره‌سازی داخلی و خارجی دستگاه

اپلیکیشن‌ها برای انجام برخی قابلیت‌ها در پلتفرمشان به تأیید دسترسی‌های ضروری و کسب اطلاعات مربوط به آن نیاز دارند؛ اما مشکلی که وجود دارد این است که اپلیکیشن‌های مخرب می‌توانند از این اطلاعات سوءاستفاده کنند. مثلا اپلیکیشن‌های مخرب پس از تأیید کاربر برای دسترسی به دوربین می‌توانند به‌طور مخفیانه، دوربین موبایل را فعال کنند و کاربر را زیر نظر داشته باشند. همچنین، اپلیکیشن‌های موسیقی برای اجرا به دسترسی به حافظه‌ی SDدارند یا شبکه‌های اجتماعی با فعال‌کردن این دسترسی می‌توانند عکس‌های آشنایانتان را در دستگاهتان ذخیره کنند؛ اما درصورتی‌که اپلیکیشن مخرب باشد، می‌تواند بدون اطلاع کاربر فایل‌هایی را در حافظه‌ی دستگاه حذف کند.

علاوه‌بر دسترسی‌های یادشده، دو گزینه‌ی دسترسی روت و ادمین نیز وجود دارد که دست افراد سودجو در آن‌ها بازتر است. برخی از اپلیکیشن‌هایی که دسترسی ادمین دارند می‌توانند رمز عبور دستگاه را تغییر دهند، تلفنتان را قفل یا به‌طور دائم داده‌های دستگاه را حذف کنند. این دسترسی را می‌توان در اپلیکیشن‌های امنیتی مشاهده کرد؛ اما ممکن است نفوذگران آن را در اپلیکیشن‌های خود نیز قرار دهند. با دسترسی ادمین در اپلیکیشن‌های امنیتی، امکان دزدیده‌شدن اطلاعات کاربر توسط هکرها وجود ندارد. علاوه‌براین، اپلیکیشن‌هایی که دسترسی روت در آن‌ها فعال می‌شود، به تمامی امکانات دستگاه دسترسی پیدا می‌کنند. سیستم اندرویدی به‌طور پیش‌فرض دسترسی روت را غیرفعال می‌کند؛ اما سازندگان بدافزارها سعی می‌کنند با روش‌های جدید، این دسترسی را در دستگاه کاربر فعال کنند.

مشاهده و تنظیم دسترسی‌های مجاز اپلیکیشن

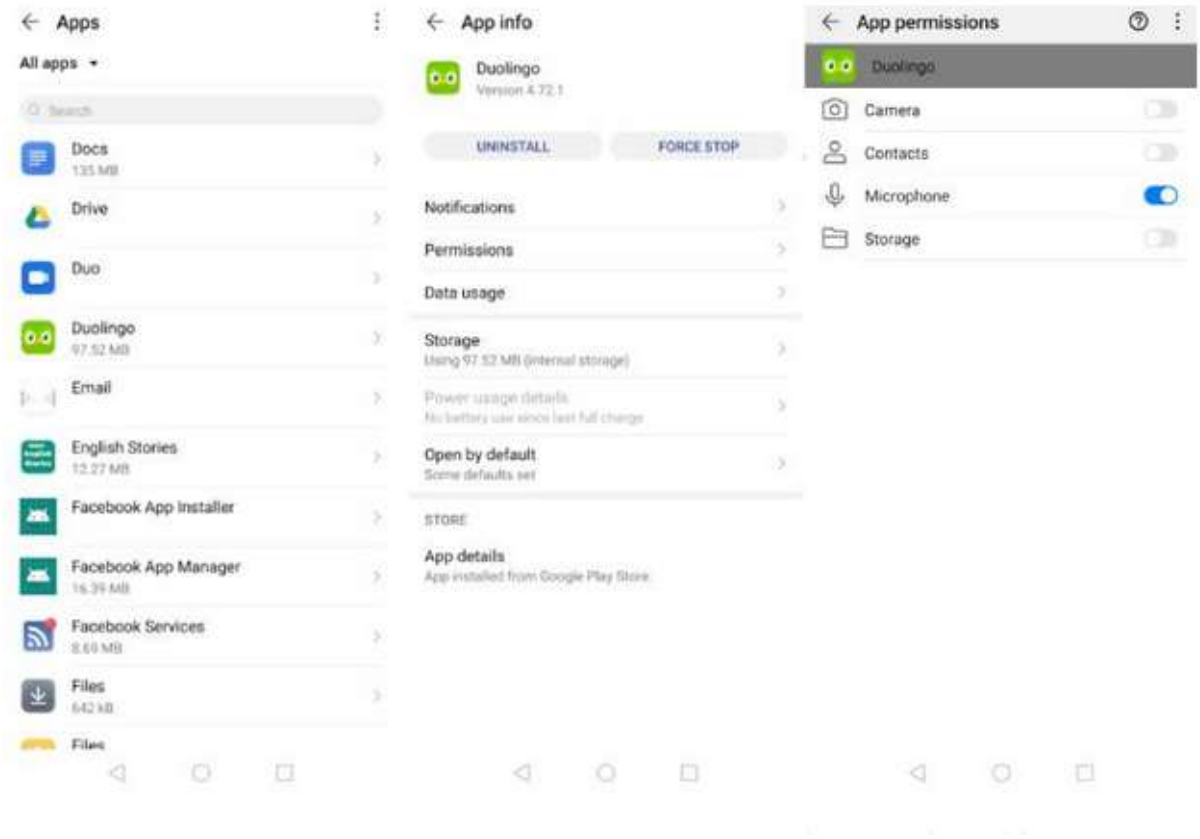
پیش از نصب اپلیکیشن، فهرستی از دسترسی‌های مجاز نشان داده می‌شود .دسترسی‌های اپلیکیشن را نیز می‌توان در قسمت دسترسی‌ها (permissions) در تنظیمات دستگاه، تنظیمات هر اپلیکیشن و نیز فروشگاه‌های اپلیکیشن‌محور مشاهده کرد. در فروشگاه‌های اپلیکیشن‌محور مانند پلی‌استور، می‌توان در قسمت توضیحات اپلیکیشن یا About this app دسترسی‌های هر اپ را پیدا کرد.

پس از نصب اپلیکیشن از قسمت دسترسی‌ها در منوی تنظیمات و تنظیمات اپلیکیشن می‌توانید گزینه‌های غیرضروری را غیرفعال کنید. در هر دو روش، برای شروع به قسمت Apps & notifications در منوی

تنظیمات گوشی یا تبلت‌تان بروید. ناگفته نماند برای انجام این کار به اندروید ۶ مارشمالو و نسخه‌های جدیدتر اندرویدی نیاز دارید.

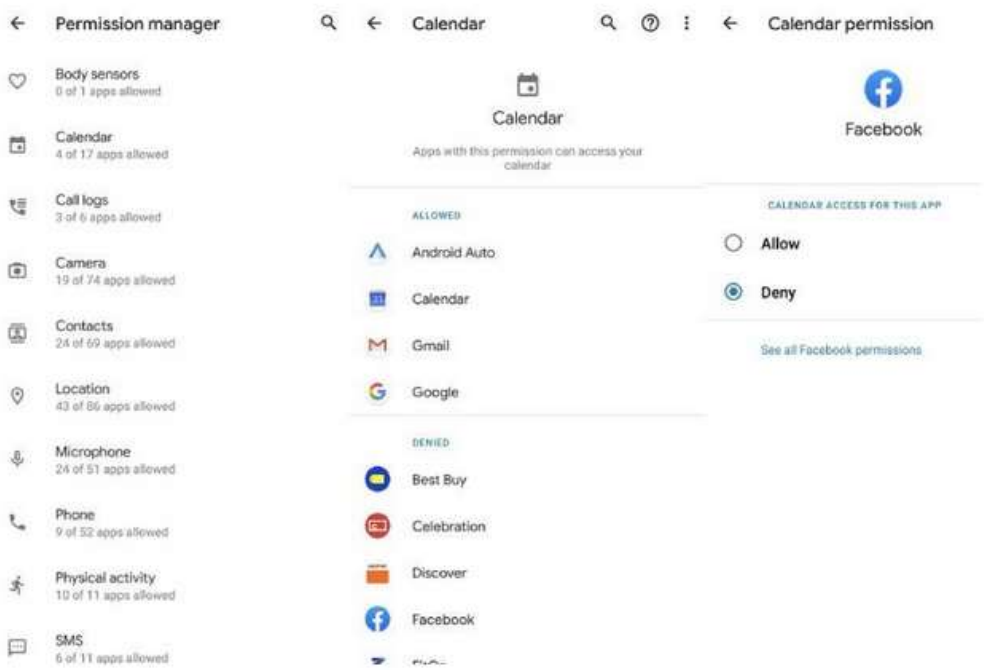
روش اول: کنترل دسترسی‌های مجاز از تنظیمات اپلیکیشن

پس از انتخاب Apps & notifications و ورود به بخش اپلیکیشن‌ها، اپلیکیشن مدنظر را انتخاب و سپس در گزینه‌یPermissions ، دسترسی‌های مجاز را فعال یا غیرفعال کنید. بدین ترتیب، بدون نصب مجدد اپلیکیشن تغییرات مدنظر را می‌توانید انجام دهید.

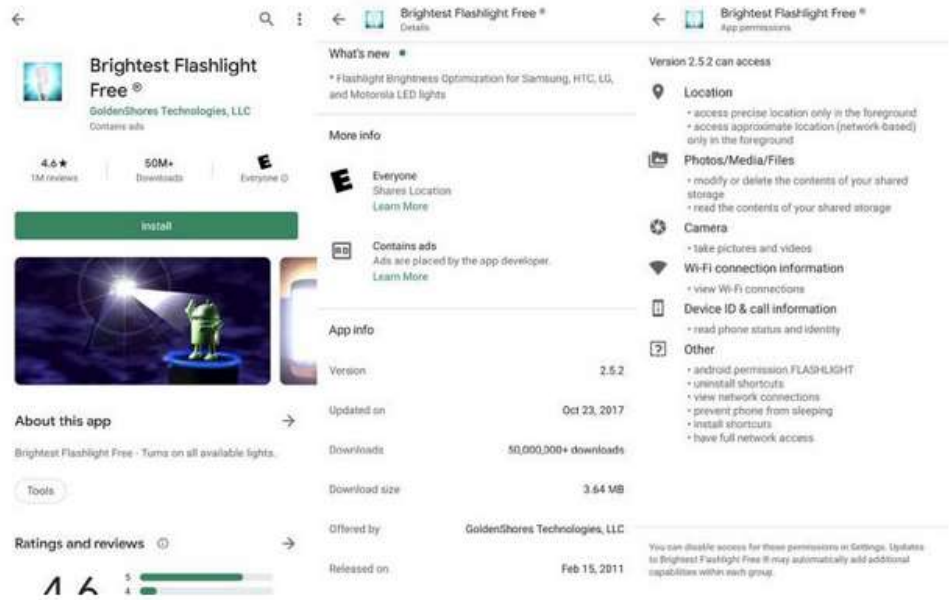


روش دوم: حذف اپلیکیشن از فهرست دسترسی‌ها

همان‌طور که پیش‌تر ذکر شد، قسمتPermissions ، گزینه‌های دسترسی را نشان می‌دهد و در هر گزینه، فهرستی از اپلیکیشن‌هایی وجود دارد که به آن گزینه دسترسی دارند. برای مثال، با ورود به بخش میکروفون می‌توانید اپلیکیشن‌هایی را ببینید که به آن دسترسی دارند. قسمت Permissions در منوی تنظیمات Apps &notifications قرار دارد؛ اما ممکن است مکان آن برای برخی از مدل‌های گوشی متفاوت باشد. با انتخاب هر گزینه، می‌توانید دسترسی اپلیکیشن مدنظر را در فهرست آن غیرفعال کنید.



یادآوری می‌شود در اپلیکیشن‌های قدیمی‌تر، امکان غیرفعال‌کردن برخی از دسترسی‌ها وجود ندارد و در اجرای اپلیکیشن باید تمام دسترسی‌ها فعال شده باشند. گاهی با درنظر گرفتن عملکرد هر اپلیکیشن، گزینه‌هایی در دسترسی‌های آن می‌بینیم که بی‌ربط هستند. مثلا اپلیکیشن‌های چراغ‌قوه برای اجرا نیازی به دسترسی به مخاطبان و میکروفون ندارند. واضح است که چنین اپلیکیشن‌هایی قصد دارند اطلاعات کاربر را جمع‌آوری کنند. در اپلیکیشن‌های اندرویدی، درخواست فعال‌سازی مجوزهای غیرضروری را زیاد مشاهده می‌کنیم و بهتر است برای امنیت بیشتر، آن‌هایی را که در عملکرد اپلیکیشن اختلال ایجاد نمی‌کنند، غیرفعال کنیم.

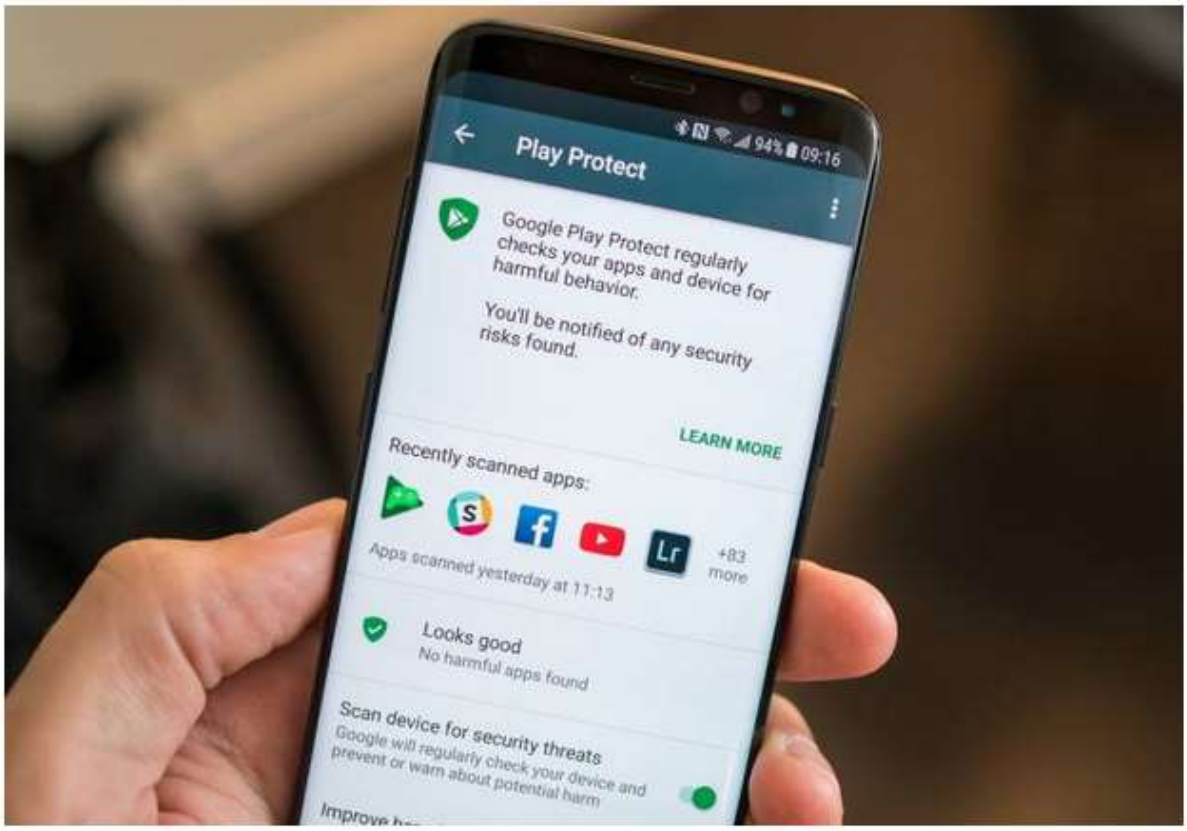


توجه داشته باشید با به‌روزرسانی‌های اپلیکیشن‌ها، گزینه‌های جدید به هر دسته‌بندی اضافه می‌شود. برای مثال، اگر اپلیکیشنی در دسترسی گزینه‌ی تلفن مجاز به «خواندن و شناسایی وضعیت تلفن» باشد، با به‌روزرسانی اپلیکیشن ممکن است «تماس با مخاطبان با هزینه‌ی کاربر» نیز به آن اضافه شود. پس درصورتی‌که کاربر دسترسی به تلفن را مجاز کرده باشد، گزینه‌های جدید در این دسترسی بدون اطلاع کاربر اضافه و فعال خواهند شد.

با دسترسی‌های مجاز می‌توانید کنترل بیشتری روی کارهای اپلیکیشن نصب‌شده داشته باشید؛ اما درصورت نداشتن اطلاعات کافی، ممکن است امنیت اطلاعاتتان تهدید شود .اپلیکیشن‌های مخرب، فهرستی از دسترسی به برنامه‌های دیگر را نشان می‌دهند که درصورت تأیید کاربر می‌توانند از اطلاعاتش سواستفاده کنند. پس بهتر است دسترسی‌های غیرمرتبط آن‌ها را غیرفعال کرد.

همچنین، توسعه‌دهندگان اپلیکیشن‌های معتبر، فهرستی از دسترسی‌ها را به کاربر نشان می‌دهند که برای اجرای اپلیکیشن لازم است؛ اما تأیید تمامی موارد الزامی نیست. در میان فهرست دسترسی اپلیکیشن‌های معتبر ممکن است گزینه‌هایی برای جمع‌آوری داده‌های گوشی وجود داشته باشد که برای اهداف تبلیغاتی استفاده می‌شود و تأیید آن‌ها اختلالی در اجرای برنامه به‌وجود نمی‌آورد.

گوگل برای امنیت بیشتر، ویژگی به‌نام Google Play Protect برای کاربرانی که اطلاعات چندانی از دسترسی‌های مجاز ندارند عرضه کرده است. این ویژگی به پلی‌استور افزوده شده و می‌تواند اپلیکیشن‌های نصب‌شده‌ی دستگاه را اسکن کند.



آگاهی و افزایش اطلاعات در زمینه‌ی حفاظت و امنیت دیجیتال اهمیت زیادی دارد. برنامه‌ها و اپلیکیشن‌های مخرب با دسترسی‌های بیشتر به برنامه‌های موبایلی می‌توانند اطلاعات کاربران را به‌دست آورند. برای مثال، اپلیکیشن‌های پیام‌رسان برای اجرا به دسترسی به مخاطبان، پیامک، دوربین و میکروفون نیاز دارند تا بتوانند تماس برقرار کنند؛ اما به دسترسی به اطلاعات سلامتی‌تان نیازی ندارند. با مدیریت صحیح دسترسی‌های مجاز می‌توان از نفوذ اپلیکیشن‌های مخرب به اطلاعات جلوگیری کرد. پیش از نصب اپلیکیشن‌ها، فهرست دسترسی‌ها را باید به دقت بررسی کنید و درصورت مشکوک‌بودن گزینه‌ها، برنامه را نصب نکنید. پس از نصب اپلیکیشن‌ها، دسترسی‌های آن را از قسمت تنظیمات بررسی و موارد غیرضروری را غیرفعال کنید.

دسترسی مجاز اپلیکیشن‌ها (App Permissions) با هدف **محافظت از اطلاعات کاربران** طراحی شده‌اند و کاربران اندروید 6 مارشمالو و بالاتر می‌توانند دسترسی‌های اپلیکیشن‌های مختلف را در گوشی هوشمند خود کنترل کرده و در صورت لزوم آنها را محدود کنند.

اپلیکیشن‌ها بخشی جدایی‌ناپذیر از **گوشی‌های هوشمند** هستند؛ برای اهداف مختلف برنامه‌های کاربردی متنوعی طراحی می‌شود که می‌تواند بسیار مفید باشد؛ برنامه‌هایی از قبیل **شبکه‌های اجتماعی، اپلیکیشن‌های پیش‌بینی وضع هوا و غیره** .با وجود این، دسترسی‌هایی که برنامه‌ها از گوشی هوشمند شما می‌خواهند، می‌تواند دردسرساز باشد. با وجود برنامه‌های متنوعی که در دسترس هستند، دانلود و نصب آنها کار ساده‌ای است اما آیا موقع نصب یک برنامه به **امنیت آن** توجه می‌کنید؟

برخی از برنامه‌ها در واقع **بدافزارهایی** هستند که به **اطلاعات کاربر** دسترسی پیدا کرده و باعث مشکلات متعددی می‌شوند. به این ترتیب بررسی ***دسترسی اندروید و مدیریت دسترسی برنامه های اندروید*** می‌تواند بسیار کمک کننده باشد.

منظور از دسترسی اندروید چیست؟

مجوزها یا دسترسی‌های اندروید می‌توانند به برنامه‌ها این امکان را بدهند که گوشی شما را تحت کنترل داشته و به **دوربین، میکروفون، پیام‌های خصوصی، مکالمات، تصاویر و غیره** دسترسی داشته باشند. این دسترسی‌ها معمولا در اولین باری که برنامه را نصب می‌کنید و برنامه **دسترسی به سخت‌افزار یا داده‌های تلفن همراه یا تبلت شما** را می‌خواهد، ظاهر می‌شوند و معمولا به **حریم خصوصی** مرتبط هستند. هر وقت که **یک برنامه‌ی جدید از Google Play** نصب می‌کنید، احتمالا **درخواست مجوز برنامه‌ها** را مشاهده خواهید کرد. برای مثال اگر یک برنامه‌ی دوربین نصب کنید حتما برای عکس گرفتن از شما **اجازه‌ی دسترسی به دوربین** را می‌خواهد.

سایر ***دسترسی های اپلیکیشن در اندروید*** می‌تواند شامل **نظارت بر موقعیت مکانی، ذخیره‌ی اطلاعات، ارسال و دریافت پیام‌ها و تماس‌ها، خواندن داده‌های حساس گزارش یا دسترسی به مخاطبین، تقویم با**

تاریخچه‌ی مرورگر شما باشد. با این حال، برنامه‌ها به طور خودکار اجازه‌ی دسترسی به هیچ کدام از این اطلاعات را ندارند و برای فعال شدن نیاز به تایید کاربر هست. بنابراین با **لغو دسترسی‌ها**، می‌توانید کنترل آنها بر گوشی خود را محدود کنید.

کنترل کننده‌ی مجوز و دسترسی اندروید چیست؟

کنترل کننده‌ی مجوزهای اندروید بخشی از سیستم عامل اندروید است که به برنامه‌ها می‌گوید به چه چیزهایی می‌توانند دسترسی داشته باشند. وقتی که **یک اپلیکیشن جدید** برای گوشی هوشمند خود دانلود می‌کنید، **کنترل کننده‌ی دسترسی های اندروید** همان چیزی است که به شما این امکان را می‌دهد که این دسترسی‌ها را قبول کنید یا رد کنید.

دسترسی‌های اندروید که باید از آنها اجتناب کنید

هنگام نصب یک برنامه باید توجه داشته باشید که دسترسی‌هایی که مورد نیاز برنامه نیست را به آن ندهید. اگر یک اپلیکیشن نباید به چیزی دسترسی داشته باشد (مانند دوربین یا لوکیشن) به آن، **مجوز دسترسی** ندهید. هنگام تصمیم گیری در مورد **پذیرش یا رد دسترسی برنامه‌ها**، حریم خصوصی خود را حتما در نظر داشته باشید .**مجوزهای سیستم اندروید** به **دو دسته‌ی دسترسی‌های طبیعی و خطرناک** تقسیم می‌شوند. اندروید به طور پیش‌فرض دسترسی‌های معمولی یا نرمال مانند دسترسی به اینترنت را به برنامه‌ها می‌دهد. این بدان دلیل است که مجوزهای معمولی نباید خطری برای حریم خصوصی یا عملکرد دستگاه شما ایجاد کنند.

از سوی دیگر مجوزهای خطرناک قرار دارد که اندروید از شما برای استفاده از آنها اجازه می‌خواهد. این **دسترسی‌های خطرناک** شامل **دسترسی به تاریخچه‌ی تماس‌ها، پیام‌های خصوصی، موقعیت مکانی، دوربین، میکروفون و غیره** می‌شود. این دسترسی‌ها ذاتا خطرناک نیستند اما امکان سوء استفاده دارند .به همین خاطر است که اندروید به شما این فرصت را می‌دهد که آنها را بپذیرید یا رد کنید. برخی از برنامه‌ها به این **دسترسی مجوزها در اندروید** نیاز دارند و در این موارد، پیش از نصب آن از ایمن بودن برنامه‌ی مورد نظر اطمینان حاصل کنید و مطمئن شوید برنامه از **یک توسعه‌دهنده‌ی معتبر** ارائه شده است.

دسترسی‌های خطرناک اندروید

اندروید **مجوزها** را در صورتی که برای حریم خصوصی و عملکرد سایر برنامه‌ها یا دستگاه شما تاثیر بگذارد، به عنوان خطرناک طبقه‌بندی می‌کند. بنابراین لازم است مراقب برنامه‌هایی باشید که مجوزی را درخواست می‌کنند که به نظر نمی‌رسد برای آنها ضروری باشد. اندروید، **9گروه دسترسی‌های خطرناک** را تعریف می‌کند. هر کدام از این **گروه‌های دسترسی‌های خطرناک** حاوی **چندین مجوز** است و با تایید یک مجوز در گروه، مجوزهای دیگر نیز تایید می‌شوند. برای مثال اگر به برنامه‌ای اجازه دهید تماس‌های شما را ببیند در واقع به آن برنامه اجازه داده‌اید که تماس نیز برقرار کند! در ادامه این **9دسترسی برنامه‌ها به اطلاعات گوشی اندروید** را بررسی می‌کنیم:

- **سنسورهای بدن**

این ویژگی **امکان دسترسی به داده‌های مربوط به سلامتی** را از مونیتورهای ضربان قلب، ردیاب‌های تناسب اندام و سایر سنسورهای خارجی فراهم می‌کند. در حالی که **برنامه‌های بدنسازی برای ارائه‌ی نکات سلامتی، بررسی ضربان قلب در طی ورزش و غیره** به این دسترسی نیاز دارند اما یک بدافزار می‌تواند از این اطلاعات شما جاسوسی کند.

- **تقویم**

اجازه دسترسی برنامه‌های اندروید به **تقویم** به این برنامه‌ها امکان **خواندن، ایجاد کردن، ویرایش کردن یا حذف رویدادهای تقویم** را می‌دهد. برنامه‌های تقویم به این دسترسی نیاز دارند تا بتوانند رویدادهای تقویمی را تنظیم کنند. در مقابل یک **بدافزار اندروید** می‌تواند بر روتین‌های شخصی شما، قرارهای ملاقات و غیره جاسوسی کند و حتی آنها را از تقویم شما حذف کند.

- **دوربین**

مجوز **دسترسی اندروید به دوربین** به برنامه‌ها اجازه می‌دهد تا از دوربین برای **عکس‌برداری و فیلم‌برداری** استفاده کنند. برنامه‌های مرتبط با دوربین به این مجوز نیاز دارند تا بتوانند از **دوربین گوشی هوشمند شما** استفاده کنند اما یک بدافزار می‌تواند به طور مخفیانه دوربین شما را روشن کرده و اتفاقاتی که در اطراف شما می‌افتد را ثبت کند.

- **مخاطبان**

این **مجوز دسترسی اندروید** به برنامه‌ها امکان می‌دهد **لیست مخاطبان** شما را بخوانند، ایجاد کنند و یا آنها را ویرایش کنند و بعلاوه به لیست همه‌ی حساب‌ها مانند فیس‌بوک، اینستاگرام، توییتر، تلگرام و غیره که روی تلفن هوشمند خود دارید دسترسی داشته باشند. با استفاده از **این مجوز دسترسی**، یک برنامه‌ی ارتباطی می‌تواند به شما کمک کند تا راحت‌تر با مخاطبان خود ارتباط برقرار کنید. البته بدافزارها نیز می‌توانند **اطلاعات مخاطبان شما** را بدزدند و سپس دوستان، خانواده و سایر افراد را با هرزنامه، انواع کلاهبرداری و غیره مورد هدف قرار دهند.

- **موقعیت مکانی**

موقعیت مکانی به برنامه‌ها مجوز می‌دهد تا با استفاده از ایستگاه‌های پایه‌ی تلفن همراه و **نقاط اتصال (مانند وای‌فای)** به **موقعیت تقریبی** شما دسترسی داشته باشند و از طریق GPS نیز **موقعیت دقیق** شما را تشخیص دهند .**برنامه‌های مسیریابی** به این دسترسی نیاز دارند و می‌توانند بسیار مفید باشند و برنامه‌های دوربین نیز می‌توانند **برچسب جغرافیایی** به تصاویر شما اضافه کنند تا بدانید عکس‌ها در کجا گرفته شده‌اند و البته برنامه‌های خرید نیز آدرس شما برای تحویل مرسوله تخمین می‌زنند. در مقابل یک **بدافزار** می‌تواند **به طور مخفیانه** به موقعیت مکانی شما دسترسی پیدا کند و حتی هکرها می‌توانند به سارقان اطلاع دهند که شما در خانه نیستید!

- **میکروفون**

میکروفون نیز کاربردهای مختلفی دارد برای مثال در برنامه‌های ارتباطی می‌توانید از **مجوز دسترسی میکروفون برای ارسال صدا** به دوستان خود استفاده کنید. با این حال باید مراقب **بدافزارها** نیز باشید چرا که به طور مخفیانه می‌توانند به صدای محیط اطراف و مکالمات خصوصی شما اطلاع پیدا کنند.

- **تماس‌ها**

این **مجوز دسترسی در اندروید** به برنامه‌ها امکان می‌دهد به **شماره تماس، اطلاعات شبکه تلفن همراه و وضعیت تماس‌های جاری** شما دسترسی داشته باشد. برنامه‌ها همچنین می‌توانند تماس برقرار کرده و یا آن را پایان دهند، گزارش‌های تماس شما را بخوانند و ویرایش کنند، پست صوتی ارسال کنند و یا حتی تماس‌ها را به شماره‌های دیگر هدایت کنند. برنامه‌های ارتباطی به طور کلی به این **مجوز دسترسی اندروید** نیاز دارند اما بدافزارها و نرم‌افزارهای جاسوسی می‌توانند مکالمات شما را بدون اجازه شنود کنند.

- **پیام‌ها**

با استفاده از این **مجوز دسترسی برنامه‌ها** می‌توانند **پیام‌های SMS** را ارسال و دریافت کنند و بخوانند. این **مجوز برای برنامه‌های ارتباطی** ضروری است و به شما امکان می‌دهد بتوانید به دوستان خود پیام بفرستید. در مقابل **بدافزارها** می‌توانند پیام‌های شما را جاسوسی کنند.

- **حافظه‌ی گوشی**

امکان دسترسی به این مجوز به برنامه‌ها اجازه می‌دهد تا به **حافظه‌ی داخلی یا کارت حافظه‌ی تلفن هوشمند** شما دسترسی داشته باشند. برای مثال یک برنامه‌ی موسیقی می‌تواند فایل‌های موسیقی را در کارت حافظه‌ی شما ذخیره کنید و یا یک برنامه‌ی شبکه‌ی اجتماعی عکس‌ها و ویدئوهای ارسال شده توسط دوستان شما را روی گوشی ذخیره کند .البته **بدافزارها** نیز می‌توانند به طور مخفیانه اسناد، موزیک‌ها، عکس‌ها و سایر فایل‌ها را بخوانند، تغییر دهند یا حذف کنند.

روش‌های تغییر دسترسی و مجوزهای برنامه‌های اندروید

برنامه‌هایی که روی گوشی هوشمند خود نصب می‌کنید **مجوز دسترسی متفاوتی** ممکن است از شما بخواهند .**فهرست دسترسی‌های مورد نیاز هر برنامه** را می‌توانید در پلی استور و در قسمت **توضیحات اپلیکیشن** مشاهده کنید .**مجوزهای برنامه‌های اندروید** را می‌توانید مدیریت کنید و در صورت لزوم آنها را تغییر دهید. در ادامه **سه روش برای تغییر دسترسی برنامه‌های اندروید** معرفی می‌کنیم.

روش اول تغییر دسترسی اندروید: بررسی دسترسی‌های برنامه پیش از نصب آن

با **بررسی مجوزهای یک برنامه پیش از نصب،** استانداردهای سخت‌گیرانه‌ی حفظ حریم خصوصی را رعایت کنید. در وهله‌ی اول لازم است دسترسی‌های مورد نیاز هر برنامه را پیش از نصب در **فروشگاه Google Play**بررسی کنید. برای این کار مراحل زیر را دنبال کنید:

1. وارد **گوگل پلی** شوید و برنامه‌ی مورد نظر خود را پیدا کرده و باز کنید.
2. به پایین بروید و روی **"درباره‌ی این برنامه "**یا **About this App**ضربه بزنید.
3. به پایین صفحه بروید و روی **App permissionsیا مجوزهای برنامه** ضربه بزنید.
4. در این قسمت می‌توانید تمام دسترسی‌هایی که برنامه از شما می‌خواهد را مشاهده کنید.

به این ترتیب می‌توانید تصمیم بگیرید که آیا به توسعه‌دهنده‌ی برنامه اعتماد دارید یا خیر و با استفاده از این مجوزهای دسترسی احساس راحتی می‌کنید یا خیر .**انتخاب و نصب برنامه‌هایی با مجوزهای مناسب،** راهی عالی برای **کنترل دسترسی برنامه‌های اندروید** از همان ابتدا است.

روش دوم تغییر دسترسی اندروید: تمام مجوزهای استفاده شده توسط یک برنامه‌ی خاص را مشاهده کنید

نگران این هستید که برنامه‌های خاص در تلفن هوشمند شما به چیزهای دسترسی دارند؟ با **بررسی مجوزهای برنامه‌ها** می‌توانید آنها را تغییر داده و **مدیریت و کنترل** بیشتری بر آنها داشته باشید. برای این کار مراحل زیر را دنبال کنید:

1. وارد بخش **تنظیمات** شده و سپس **Apps & notifications**را باز کنید.
2. در این صفحه برنامه‌ای که می‌خواهید دسترسی‌های آن را کنترل کنید را پیدا کرده و باز کنید.
3. گزینه‌ی **Permissions**را انتخاب کنید.
4. در این قسمت می‌توانید تمام **دسترسی های برنامه اندروید** مورد نظر را مشاهده کنید و برای تغییر یک اجازه تنها کافی است آن را لمس کنید.

5. شما می‌توانید دسترسی‌هایی که ضروری نیستند را حذف کنید.

برنامه‌های گوشی همراه شما برای درست کار کردن به برخی از مجوزها نیاز دارند. اگر دسترسی **گوگل مپ (Google Map)**به موقعی مکانی خود را لغو کنید، این برنامه نمی‌تواند به شما جهات را نشان دهد و بعلاوه نمی‌تواند جستجوهای شما روی نقشه را بر اساس موقعیت مکانی شما انجام دهد.

روش سوم تغییر دسترسی اندروید: مشاهده‌ی همه‌ی برنامه‌هایی که از یک مجوز خاص استفاده می‌کنند

اگر ترجیح می‌دهد نگاهی به **لیست *دسترسی اپلیکیشن در اندروید*** بیاندازید و دسترسی خاصی مانند مکان یا مخاطبین را مشاهده کنید، این روش می‌تواند در حفظ حریم خصوصی در اندروید برای شما بسیار کاربردی باشد. در ادامه نحوه‌ی **دسترسی به لیست مجوزهای برنامه** برای دیدن همه‌ی برنامه‌هایی که از یک مجوز خاص استفاده می‌کنند را شرح می‌دهیم:

1. وارد **تنظیمات** و سپس **Apps & notifications**شوید.
2. روی **مدیریت مجوزها (Permission manager)** کلیک کنید تا برنامه‌ی **کنترل‌کننده‌ی مجوزهای اندروید (Android permission controller app)** را باز کنید.
3. در صفحه‌ی باز شده روی **مجوزهای خاص** برنامه‌ها کلیک کنید (مانند مجوز **موقعیت مکانی یا Location** و غیره)
4. در این قسمت می‌توانید اپلیکیشن‌هایی که به موقعیت مکانی شما دسترسی دارند را مشاهده کنید. برای حذف دسترسی روی هر کدام از آنها کلیک کنید.

مجوزهای دسترسی برنامه‌های اندروید و امنیت تلفن هوشمند شما

حفاظت از اطلاعات تلفن‌های هوشمند یکی از روش‌های امنیتی است که نمی‌توان آن را نادیده گرفت. با نظارت بر برنامه‌هایی که نصب می‌کنید و **بررسی مجوزهای دسترسی اندروید** این امنیت را بیشتر حفظ خواهید کرد چرا که **بدافزارها و برنامه‌های مخرب** با **دسترسی‌های غیرمجاز** می‌توانند اطلاعات خصوصی کاربران را به دست آورده و از آنها سوء استفاده کنند.

با ***مدیریت دسترسی برنامه های اندروید***، از جمله موقعیت مکانی، تماس‌ها، پیامک‌ها و غیره **از نفوذ بدافزاها به اطلاعات شخصی خود** پیشگیری کنید و البته پیش از نصب برنامه‌ها از **ایمن بودن آنها** اطمینان حاصل کنید. گاهی اوقات نیز لازم است سری به **تنظیمات و مجوزهای برنامه‌های مختلف** بزنید و موارد غیرضروری یا مشکوک را حذف کنید.

در ادامه‌ی این گزارش با مفاهیمِ عمیقِ مربوط به مجوزها و امضاهای برنامه‌های اندرویدی که عموما توسط برنامه‌نویسان به کار گرفته می‌شوند، بحث خواهیم کرد.

مجوزهای سیستم

آندروید یک سیستم عامل با قابلیت مجزا سازی است که در آن هر برنامه با هویت مجزا اجرا می‌شود (ID کاربر لینوکس و ID گروهی). همچنین بخش‌هایی از سیستم نیز هویت های متمایز دارند. در نتیجه لینوکس برنامه های کاربردی را از یکدیگر و از سیستم جدا می‌کند.

ویژگی‌های امنیتی ریز اضافی از طریق مکانیزم "مجوز" مهیا شده است که محدودیت‌هایی در اجرای عملیات‌های خاص که می‌تواند در یک فرآیند مخصوص انجام شود ایجاد می‌کنند، و همچنین این ویژگی‌ها در مجوزهای هر URI برای دادن دسترسی موقت به بخش خاصی از داده‌ها محدودیت ایجاد می‌کنند.

این سند شرح می‌دهد که چگونه سازندگان نرم افزار می‌توانند از ویژگی‌های امنیتی ارائه شده توسط آندروید استفاده کنند. اطلاعات عمومی بیشتر در مورد امنیت آندروید در آرشیو پروژه آندروید اوپن سورس وجود دارد.

ساختار امنیت

نقطه ذظر اصلی طراحی معماری امنیتی آندروید این است که هیچ برنامه، به‌طور پیش فرض است، اجازه انجام هرگونه عملیات که تاثیر منفی روی برنامه‌های کاربردی دیگر، سیستم عامل، و یا کاربر را داشته باشد را نمی‌دهد. این شامل خواندن و نوشتن اطلاعات خصوصی کاربر (مانند اطلاعات تماس یا ایمیل)، خواندن و نوشتن فایل‌های برنامه‌های دیگر و انجام دسترسی به شبکه، نگهداری بیدار دستگاه، و غیره می‌باشد.

از آنجا که هر برنامه آندروید در یک فرایند sandbox کار می‌کند، برنامه‌های کاربردی باید منابع و اطلاعات را به اشتراک بگذارند. آنها این کار را با درخواست مجوز برای داشتن قابلیت‌های اضافه که توسط sandbox عمومی ارائه نشده است انجام می‌دهند. برنامه‌ها مجوز مورد نیاز را به صورت استاتیکی درخواست می‌کنند و سیستم آندروید کاربر را در زمان نصب برنامه برای رضایت از این موضوع مطلع می کند. آندروید هیچ مکانیزمی برای اعطای مجوز به صورت پویا (در زمان اجرا) نمی‌دهد چون این باعث پیچیده شدن کار کاربر و به ضرر امنیت است.

sandbox یک برنامه بستگی به تکنولوژی استفاده شده برای ساخت آن برنامه ندارد. به‌طور خاص DALVIK VM یک مرز امنیتی نیست، و هر برنامه‌ای می‌تواند کد اصلی (native) اجرا کند (نگاه کنید به آندروید NDK). همه نوع از برنامه‌های کاربردی - جاوا، بومی و هیبرید - با یک روش ساندباکس شده اند و درجه امنیت آنها یکسان است.

امضای برنامه

همه APK ها (فایل‌های APK) باید با یک گواهی که رمز آن پیش سازندگان است امضا شوند. این گواهی نویسنده نرم افزار را شناسایی می‌کند. گواهی نیازی به امضای مراجع معتبر ندارند بلکه می‌توان برای برنامه‌های کاربردی آندروید از گواهی‌های خود معتبر استفاده کرد که کاملا مجاز و معمول هستند. هدف از گواهی در آندروید این است که سازندگان برنامه کاربردی مشخص شوند. این اجازه می‌دهد تا سیستم دسترسی به برنامه‌های کاربردی به مجوزهای در سطح امضا را رد یا قبول کند و همچنین اجازه می‌دهد تا به درخواست یک برنامه برای گرفتن هویت لینوکس یک برنامه دیگر پاسخ رد یا قبول دهد.

شناسه کاربری و دسترسی به فایل

در زمان نصب، آندروید به طور جداگانه یک شناسه کاربری لینوکس به هر پکیج می‌دهد. این هویت در تمام طول عمر دستگاه در پکیج ثابت می‌ماند. در یک دستگاه متقاوت، همان پکیج ممکن است UID های متقاوتی داشته باشد؛ آنچه مهم است این است که هر پکیج دارای یک UID مجزا در هر دستگاه است.

از آنجا که ملزومات امنیت در سطح فرآیند اتفاق می افتند، کد هیچ دو پکیجی در یک فرایند مشترک اجرا نمی‌شود، چرا که می‌بایست آنها به عنوان‌های کاربرهای مختلف لینوکس اجرا شوند. شما می‌توانید ویژگی sharedUserId را در برچسب آشکارساز AndroidManifest.xml هر پکیج استفاده کنید تا یک شناسه کاربری مشترک به آنها اختصاص دهید. با انجام این کار، برای اهداف امنیتی دو پکیج به عنوان یک برنامه شناخته می‌شوند که ID و مجوزهای فایل یکسانی دارند. توجه داشته باشید که به منظور حفظ امنیت، تنها به دو برنامه‌های کاربردی امضا شده با امضای یکسان یک ID مشترک داده می‌شود.

هر گونه داده‌های ذخیره شده توسط نرم افزار اختصاص داده خواهد شد به یک شناسه کاربری و به‌طور معمول در دسترس پکیج‌های دیگر قرار نخواهد گرفت. هنگام ایجاد یک فایل جدید با

getSharedPreferences (String, int)

openFileOutput(String, int)

یا

openOrCreateDatabase(String, int, SQLiteDatabase.CursorFactory)

شما می‌توانید از فلگ‌های

MODE_WORLD_READABLE

و یا

MODE_WORLD_WRITEABLE

استفاده کنید تا اجازه دهید به پکیج‌های دیگر که فایل را بخوانند یا بنویسند (write). هنگام تنظیم این پرچم‌ها، فایل هنوز متعلق به برنامه شماست، اما مجوز خواندن و یا نوشتن عمومی برای هر برنامه‌ای که آن را بتواند ببیند صادر شده است.

مجوز استفاده

یک برنامه پایه آندروید هیچ‌گونه مجوزی به‌طور پیش فرض ندارد، به این معنی که آن نمی‌تواند هیچ تأثیر منفی روی کار کاربر و یا روی اطلاعات بر روی دستگاه داشته باشد. برای استفاده از ویژگی‌های محافظت از دستگاه، شما باید در AndroidManifest.xml خود یک یا چند برچسب <uses-permission> برای گرفتن مجوزهایی که برنامه شما نیاز دارد استفاده کنید.

به عنوان مثال، یک برنامه که نیاز به نظارت بر پیام‌های SMS های دریافتی دارد برچسب‌های زیر را می‌خواهد :

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
  package="com.android.app.myapp" >
  <uses-permission android:name="android.permission.RECEIVE_SMS" />
  ...
</manifest>
```

در زمان نصب برنامه ، مجوزهای لازم توسط نصب کننده به آن داده می‌شود. البته مجوزهایی که بر اساس امضا (قرارداد) برنامه می‌توان درخواست داد و یا مجوزهایی که کاربر می‌تواند با برنامه ارتباط دو طرفه داشته باشد. وقتی یک برنامه در حال اجرا است هیچ بررسی بر روی کاربر انجام نمی‌شود. همچنین یک اپلیکیشن زمانی مجوز می‌گیرد که نصب شده باشد و بتواند از آن ویژگی به صورت مطلوب استفاده کند. یا اینکه کلا هیچ مجوزی داده نمی‌شود و هر تلاشی برای استفاده از فیچرهای برنامه بی‌فایده خواهد بود.

اغلب اوقات یک مشکل مجوز منجر به SecurityException (استثنای امنیتی) می‌شود که به برنامه اعمال می‌شود. با این حال، این اتفاق هر جایی صورت نمی‌پذیرد. به عنوان مثال، روش sendBroadcast(Intend) مجوزها را چک می‌کند که اطلاعات به گیرنده‌ها تحویل داده شده است، اگر مشکل مجوز وجود داشته باشد شما یک پیغام خطا دریافت خواهید کرد. تقریبا در همه موارد یک مشکل مجوز در لاگ سیستم چاپ خواهد شد.

با این حال، در یک وضعیت کاربر معمولی (مانند زمانی که برنامه از Google Play Store نصب شده باشد) ، نرم افزار نمی‌تواند نصب شود اگر کاربر مجوزهای لازم نرم افزار را نداشته باشید. بنابراین شما به طور کلی لازم نیست که نگران خطای زمان اجرا باشید که به دلیل نبود مجوز رخ داده است. به خاطر اینکه برنامه‌ای که نصب شده می‌بایست مجوزهای لازم را داشته باشد.

مجوزهای ارائه شده توسط سیستم عامل Android را می‌توان در Manifest.permission یافت. هر برنامه نیز ممکن است مجوزهای خواص خود را لازم داشته باشد، پس این یک لیست جامع از همه مجوزهای لازم نیست.

* در حین اجرای برنامه شما یک مجوز خاص ممکن است در تعدادی از نقاط کار کند:

* در زمان فراخوانی سیستم، برای جلوگیری از یک برنامه از اجرای عملکردهای خاص.

* هنگامی که شروع یک فعالیت، برای جلوگیری از راه‌اندازی کار برنامه‌های دیگر.

* در ارسال و دریافت پخش برنامه، کنترل می کند چه کسی می‌تواند پخش شما را دریافت و یا چه کسی می‌تواند پخش خود را برای شما ارسال کند.

* هنگام دسترسی و اجرای برنامه بر روی محتویات مهیا کننده (سرور).

* زمان اتصال و یا شروع یک سرویس.

توجه: با گذشت زمان، ممکن است محدودیت‌های جدید به پلت فرم اضافه شود به‌طوری که، به منظور استفاده از API های خاص، برنامه شما مجوزی درخواست کند که قبلا نیازی نداشت. از آنجا که فرض می شود برنامه‌های موجود دسترسی آزادی به API ها دارند، آندروید ممکن است درخواست مجوز جدید برای آشکارسازی برنامه نماید که برای جلوگیری از خرابی برنامه در نسخه جدید پلت فرم است. آندروید تصمیم می گیرد که آیا یک برنامه ممکن است احتیاج به مجوز بر اساس ارزش ارائه شده برای ویژگی targetSdkVersion داشته باشد یا خیر. اگر ارزش پایین تر از نسخه‌های باشد که در آن مجوز اضافه شده است ، آندروید مجوز را اضافه می‌کند.

به‌عنوان مثال، مجوز WRITE_EXTERNAL_STORAGE در سطح API 4 برای محدود کردن دسترسی به فضای ذخیره سازی مشترک اضافه شده است. اگر targetSdkVersion شما 3 و یا کمتر است، این مجوز به برنامه شما در نسخه های جدیدتر آندروید اضافه می شود.

مراقب باشید که اگر این اتفاق برای برنامه شما بیافتد، لیست برنامه های شما در Google Play مجوزهای لازم را نشان می دهد حتی اگر برنامه شما ممکن است به آنها واقعا نیاز نداشته باشد.

برای جلوگیری از این موضوع و حذف مجوزهای پیش فرض شما لازم نیست ، همیشه targetSdkVersion خود را به روز رسانی کنید. شما می‌توانید ببینید که چه مجوزهایی را در هر نسخه در اسناد Build.VERSION_CODES اضافه شده‌اند.

درخواست و اجرای مجوزها

برای اجرای مجوزهای خود، شما باید اول آنها را در AndroidManifest.xml خود با یک یا چند برچسب <permission> فراخوانی کنید.

به عنوان مثال ، یک برنامه ای که می خواهد کنترل کند چه کسی می تواند یکی از فعالیت های خود را شروع کند، می تواند یک مجوز برای این عملیات به شرح زیر اعلام کند:

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
  package="com.me.app.myapp" >
  <permission
android:name="com.me.app.myapp.permission.DEADLY_ACTIVITY"
    android:label="@string/permlab_deadlyActivity"
    android:description="@string/permdesc_deadlyActivity"
    android:permissionGroup="android.permission-group.COST_MONEY"
    android:protectionLevel="dangerous" />
  ...
</manifest>
```

ویژگی <protectionLevel> مورد نیاز است برای گفتن این که سیستم چگونه کاربر را مطلع می‌سازد که برنامه ها به مجوز احتیاج دارند و یا چه کسی مجاز به داشتن مجوز است، این موارد در اسناد پیوست شده تشریح شده‌اند.

ویژگی <permissionGroup> اختیاری است، و تنها برای کمک به نمایش مجوز سیستم به کاربر می‌باشد. شما معمولا می خواهید این را به صورت گروه سیستم استاندارد (ذکر شده در android.Manifest.permission_group) تنظیم نمایید و یا به صورت نادر خودتان تعریف کنید. ترجیح داده می‌شود که از یک گروه موجود استفاده شود، چرا که نمایش UI برای کاربر ساده تر می‌کند.

توجه داشته باشید که هر دو برچسب و شرح باید برای مجوز عرضه شده باشد. اینها منابع رشته‌ای هستند که می‌توانند به کاربر نمایش داده شوند زمانی که آنها درحال دیدن لیستی از مجوزها android:label() یا جزییات یک مجوز (android:description) هستند. یک برچسب باید کوتاه باشد، چند کلمه برای توصیف قسمت اصلی قابلیت مجوز. توضیحات باید چند جمله توصیفی از آنچه که مجوز اجازه می‌دهد تا دارنده آن انجام دهد باشد. قرار ما برای توصیفات دو جمله است، اولی توصیف کننده مجوز، و دومی اخطار به کاربر در مورد اینکه چه اتفاق بدی می تواند بیافتد اگر یک برنامه دارای مجوز شود.

در اینجا یک مثال از یک برچسب و توضیح برای مجوز CALL_PHONE وجود دارد:

```
<string name="permlab_callPhone">directly call phone numbers</string>
  <string name="permdesc_callPhone">Allows the application to call
     phone numbers without your intervention. Malicious applications may
     cause unexpected calls on your phone bill. Note that this does not
     allow the application to call emergency numbers.</string>
```

<string name="permlab_callPhone"> شماره تلفن تماس مستقیم

<string name="permdesc_callPhone"> اجازه می‌دهد تا برنامه بدون دخالت شما به‌شماره تلفنی تماس بگیرد. برنامه‌های مضر ممکن باعث تماس‌های غیر منتظره شوند. توجه داشته باشید که این اجازه نمی‌دهد تا برنامه به شماره‌های اضطراری تماس بگیرد.

شما می‌توانید نگاه کنید به مجوزهایی که در حال حاضر در سیستم با اپلیکیشن Settings و فرمان پوسته adb shell pm list permissions تعریف شده‌اند. برای استفاده از اپلیکیشن Settings بروید Settings > Applications. یک اپلیکیشن انتخاب کنید و به پایین حرکت کنید تا مجوزهای آن را ببینید. برای سازندگان، گزینه 'adb '-s مجوزها را در یک فرم شبیه به نحوه دیده شده برای کاربر نشان می دهد:

```
$ adb shell pm list permissions -s
All Permissions:

Network communication: view Wi-Fi state, create Bluetooth connections, full
Internet access, view network state

Your location: access extra location provider commands, fine (GPS) location,
mock location sources for testing, coarse (network-based) location

Services that cost you money: send SMS messages, directly call phone numbers

...
```

اجرای مجوز ها در AndroidManifest.xml

مجوزهای سطح بالا دسترسی به تمام اجزای سیستم و یا برنامه ای که می تواند از طریق AndroidManifest.xml شما اجرا شود را محدود می کند. تمام چیزی که این نیاز دارد در ویژگی android:permission بر روی یک قطعه مطلوب وجود دارند، این قطعه طوری نام گذاری شده است که نشان دهنده مجوزی است که استفاده می شود برای کنترل دسترسی به آن.

مجوزهای Activity(اعمال شده به برچسب <activity>) کسی را محدود می‌کند که می‌تواند فعالیت‌های مرتبطی را شروع کند. مجوز در طول (Context.startActivity) و

Activity.startActivityForResult) بررسی می‌شود؛ در صورتی که درخواست کننده مجوز لازم را نداشته باشد SecurityException از تماس (یا فراخوانی) خارج می شود.

مجوزهای Service(اعمال شده به برچسب <service>) کسی را محدود می‌کند که می‌تواند فعالیت‌های مرتبطی را شروع کند یا پیوند بزند. مجوز در طول (Context.startService)، (Context.stopService) و (Context.bindService) بررسی می‌شود؛ در صورتی که درخواست کننده مجوز لازم را نداشته باشد SecurityException از تماس (یا فراخوانی) خارج می‌شود.

مجوزهای BroadcastReceiver(اعمال شده به برچسب <receiver>) کسی را محدود می‌کند که می‌تواند پخش برنامه را به گیرنده مرتبطی ارسال کند. مجوز پس از بازگشت (Context.sendBroadcast) بررسی می‌شود، زمانی که سعی می کند برنامه پخش را به یک گیرنده بفرستد. در نتیجه، یک خطای مجوز منجر به پیامی نمی‌شود که به تماس گیرنده برگشت داده شود؛ تنها این برنامه است که به گیرنده مد نظر ارائه نخواهد شد. به همان صورت، یک مجوز می‌تواند به (Context.registerReceiver) داده شود برای کنترل کسی که می‌تواند به یک گیرنده محدود شده با برنامه نویسی شده برنامه پخشی بفرستد. از طرف دیگر، مجوز زمانی می‌تواند داده شود که (Context.sendBroadcast) فراخوانی می شود تا ابجکت‌های BroadcastReceiver که مجاز به دریافت پخش هستند را محدود کند (پایین را ببینید).

مجوزهای ContentProvider (اعمال شده به برچسب <provider>) کسی را محدود می‌کند که می‌تواند دسترسی داشته باشد به داده‌ها در ContentProvider. (ارائه دهندگان محتوا امکانات امنیتی اضافی مهمی دارند که در دسترس آنهایی است که با URI permissions نام گذاری شده اند. بعدا درمورد آنها شرح داده می شود). بر خلاف اجزای دیگر، دو ویژگی جدا برای مجوز وجود دارد که شما می توانید ست کنید: android:readPermission کسی را محدود می کند که می تواند داده ها را از ارائه دهنده بخواند android:writePermission کسی را محدود می کند که می تواند در آن بنویسد. توجه داشته باشید که اگر یک ارائه دهنده با هر دو مجوز خواندن و نوشتن محافظت شود، فقط داشتن مجوز نوشتن به این معنا نیست که شما می توانید از یک ارائه دهنده بخوانید. وقتی شما اولین بار به ارائه دهنده متصل می شوید (اگر شما هر دو مجوز را مدارید ،SecurityException رخ می دهد)، و یا وقتی شما عملیاتی را بر روی ارائه دهنده انجام می دهید مجوز ها چک می شوند. برای استفاده از (ContentResolver.query) نیاز به داشتن مجوز خواندن است. برای استفاده از (ContentResolver.insert)، (ContentResolver.update)، (ContentResolver.delete) نیاز به مجوز نوشتن است. در تمام این موارد، نداشتن مجوز منجر به SecurityException می‌شود.

اجرای مجوزها در هنگام ارسال برنامه‌های پخش شدنی (Broadcast)

علاوه بر مجوزی که مشخص می‌کند چه کسی می‌تواند به BroadcastReceiver چیزی بفرستد (در بالا توضیح داده شد)، شما همچنین می‌توانید مجوز مورد نیاز در هنگام ارسال پخش را مشخص کنید. با فراخوانی (Context.sendBroadcast) با یک رشته مجوز، نیاز است که نرم افزار گیرنده یک مجوز به منظور دریافت پخش داشته باشد.

توجه داشته باشید که هر دو یک گیرنده و فرستنده می‌توانند مجوز نیاز داشته باشند. هنگامی که این اتفاق می‌افتد، بررسی هر دو مجوز بایستی مثبت باشند تا برنامه مد نظر پخش به مقصد ارسال شود.

اجرای دیگر مجوزها

مجوزهای قراردادی کوچک می‌توانند در هر فراخوانی داخل سرویس اجرا شوند. این با استفاده از روش (Context.checkCallingPermission) انجام می‌شود. شما فراخوانی کنید با یک رشته مجوز مورد نظر و آن یک عدد صحیح برمی‌گرداند که نشان می‌دهد آیا این مجوز به روند فراخوانی فعلی اعطا شده است یا نه. توجه داشته باشید که این تنها می‌تواند زمانی استفاده شود که شما یک فراخوانی را اجرا می‌کنید که از فرآیند دیگر می‌آید، معمولا از طریق یک رابط IDL منتشر شده از یک سرویس و یا به طریقی به فرایند دیگری داده می‌شود.

تعدادی از دیگر راه‌های مفید برای بررسی مجوز دسترسی وجود دارند. اگر شما PID پروسه‌های دیگر را داشته باشید، می‌توانید از روش زمینه Context.checkPermission (String, int, int) برای بررسی مجوز در برابر آن PID استفاده کنید. اگر شما نام مجموعه‌ای از برنامه‌های دیگر را دارید، می‌توانید از روش PackageManager مستقیم PackageManager.checkPermission(String, String) برای فهمیدن این که آیا این بسته‌بندی خاص دارای مجوز خاص می‌باشد.

مجوزهای URI

سیستم مجوز استانداردی که تا کنون شرح داده شد اغلب کافی نیست وقتی که با تامین کنندگان محتوا استفاده می‌شود. ارائه دهنده محتوا ممکن است بخواهد از خود با مجوز خواندن و نوشتن محافظت کند، در حالی که مشتریان مستقیم آن نیز نیاز دارند به دادن URI های خاص به یک برنامه دیگر برای کار به روی آنها. به عنوان نمونه فایل پیوست در یک برنامه پست الکترونیکی را می‌توان نام برد. دسترسی به پست الکترونیکی باید با مجوز محافظت انجام شود، چون این داده حساس کاربر است. با این حال، اگر یک URI به پیوست تصویر یک نمایشگر تصویر داده شده است، آن نمایشگر تصویر مجوز باز کردن فایل پیوست نخواهد داشت چون هیچ دلیلی برای داشتن یک مجوز برای دسترسی به تمام ایمیل ندارد.

راه حل این مشکل مجوز برای هر URI است: در هنگام شروع یک فعالیت و به نتیجه رسیدن یک فعالیت، تماس گیرنده می‌تواند Intent.FLAG_GRANT_READ_URI_PERMISSION و / یا Intent.FLAG_GRANT_WRITE_URI_PERMISSION را تنظیم کند. این مجوز فعالیت دریافت اطلاعات را برای دسترسی به داده‌های خواص از URI در مقصد را می‌دهد بدون در نظر گرفتن که آیا آن مجوز دسترسی به اطلاعات ارائه دهنده محتوا دارد یا خیر.

این مکانیزم اجازه می‌دهد تا یک مدل مشترک قابلیت. سبک که در آن تعامل با کاربر (باز کردن یک پیوست، انتخاب یک تماس از یک لیست، و غیره) باعث دادن مجوز ریز می‌شود. این می‌تواند یک امکان کلیدی برای کاهش مجوز مورد نیاز توسط برنامه‌های کاربردی شود یعنی مجوز تنها به آنهایی که به طور مستقیم به رفتار آنها مربوط می‌شود داده می‌شود.

با این حال اعطای مجوزهای URI ریز نیاز به همکاری با ارائه دهنده محتوا دارد که URI ها را نگه می‌دارند. به شدت توصیه می‌شود که ارائه دهندگان محتوا این امکانات را پیاده سازی کنند، و اعلام کنند که آنها پشتیبانی می‌کنند از طریق ویژگی android:grantUriPermissions یا برچسب <grant-uri-permissions>.

اطلاعات بیشتر در روش‌های

(Context.revokeUriPermission) ,(Context.grantUriPermission)

و

(Context.checkUriPermission)

یافت می‌شود.

مروری بر روش های امضاء (Sign)برنامه های اندرویدی

توسعه دهندگان اندروید، در مراحل پایانی پروژه و قبل از انتشار برنامه در یکی از مارکت های موجود مانند گوگل پلی ، کافه بازار و ...مسئله ی امضا کردن برنامه از طریق **کلید** (Keystore)رو تجربه کرده اند. امضا کردن برنامه باعث می شود مطمئن شویم که تنها افراد مجاز بتوانند برنامه را در آینده بروز رسانی کنند و بنابراین با این کار از دسترسی افراد غیر مجاز جهت بروزرسانی برنامه جلوگیری می کنیم. با این حال، به علت اینکه کلید برنامه ها، عضو مهمی از آنها محسوب می شود، در شرایطی خاص، ممکن است توسعه دهنده را دچار مشکلات زیادی کند. به علت معایب روش فعلی امضا کردن برنامه ها (که در ادامه به آن اشاره خواهیم کرد)، روشی دیگری جهت امضا کردن برنامه ها توسط گوگل پلی (Google Play App Signing) ارائه شده تا فرایند انتشار برنامه ها **ساده تر** و البته **امن تر** صورت گیرد. متاسفانه تا لحظه ی نگارش این مقاله، این روش فقط برای انتشار برنامه در مارکت رسمی گوگل (Google Play)ارائه شده و مارکت های

ایرانی از این روش پشتیبانی نمی کنند. در این مقاله، قصد داریم این روش جدید به همراه مزایا و معایب آن را معرفی کنیم.

روش جدید امضا کردن برنامه:(Google Play App Signing)

این روش که در واقع یک فرایند جدید و اختیاری برای توسعه دهندگان محسوب می شود، کل فرایند امضای برنامه را به گوگل واگذار می کند. به محض اینکه کلید امضای خود را به همراه نسخه برنامه به کنسول گوگل پلی معرفی کنید، گوگل فرایند امضاء برنامه ارسالی را برای انتشار برنامه انجام می دهد و در واقع برنامه ی ارسالی را برای ارائه به کاربران آماده سازی و امضاء می کند. صفر تا صد این فرایند در روش قبلی برعهده توسعه دهنده بوده است .

معایب روش قدیمی امضاء کردن برنامه ها

با وجود اینکه روش قدیمی امضا کردن برنامه ها هنوز به خوبی جوابگوی توسعه دهندگان هست و توسط همه ی مارکت های انتشار برنامه از جمله گوگل پلی پشتیبانی می شود، خطرهایی در این روش وجود دارد که می تواند نگرانی هایی را برای توسعه دهندگان به همراه داشته باشد:

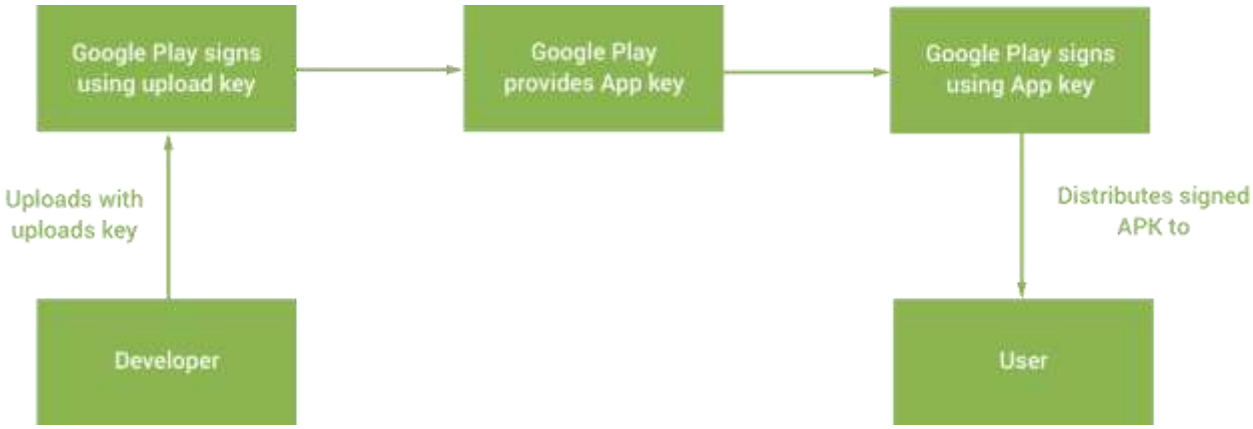
- اگر شما کلید امضا برنامه را گم کنید، هرگز نمی توانید برنامه ی خود در بروز رسانی کنید. شاید کامپیوتر شما خراب شود و هیچ بکاپی وجود نداشته باشد، در این شرایط نمی توانید برنامه ی خود را بروزرسانی کنید. مجبور هستید برنامه خود را با یک Package Name متفاوتی آپلود کرده و همه چیز را از صفر شروع کنید. یک تجربه بسیار تلخ که ممکن است گریبانگیر هر توسعه دهنده ای شود.
- کلید شما می تواند توسط اشخاصی با اهداف خرابکارانه، ربایده شود. در این حالت هر شخصی که کلید را داشته باشد، می تواند برنامه شما را بدون اجازه ی شما بروز رسانی کند و متاسفانه در این صورت، هیچ راهی برای پس گرفتن این دسترسی از شخص مخرب وجود ندارد.

بزرگترین مزیت استفاده از روش جدید امضای برنامه این است که زیرساخت گوگل، مسئولیت امضای برنامه را بر عهده خواهد گرفت و این به معنای **امنیت** هرچه بیشتر است. زمان استفاده از این روش، 2 کلید متفاوت برای فرایند امضای برنامه استفاده می شود:

- **کلید :App Signing Key** کلیدی که توسط گوگل برای امضای نسخه برنامه، قبل از انتشار استفاده می شود.
- **کلید :Upload Key** کلیدی که توسط توسعه دهنده استفاده می شود و می بایست هنگام بارگذاری نسخه برنامه، به کنسول گوگل پلی ارائه شود.

همانطور که مشاهده می کنید، توسعه دهندگان هنوز می بایست یک نسخه از کلید را نزد خود نگهداری کنند. اما تفاوت این روش این است که کلید نزد توسعه دهنده(**Upload Key**)، برای امضای نسخه ای

که قرار است منتشر شود، استفاده نمی شود و صرفا برای شناسایی مالک برنامه که قصد آپلود برنامه را دارد به کار می رود. به همین علت گوگل هر زمانی می تواند آن را جایگزین کند. اگر کلید مفقود یا ربابیده شود، دیگر هیچ شخصی ثالثی دسترسی بروزرسانی برنامه را نخواهد داشت و گوگل به راحتی می تواند کلید قبلی را غیر فعال کرده و کلید دیگری را برای استفاده مجدد بکار گیرد.(روش انجام کار در انتهای مقاله ذکر شده است)



روند امضاء شدن برنامه در روش جدید

همانطور که در شکل می بینید، شما میتوانید کلید نزد خود (**Upload Key**)را به عنوان یک کلید معتبر(و نه کلید اصلی برنامه) در نظر بگیرید. این کلید به توسعه دهنده فقط **اجازه ی بارگذاری** نسخه های برنامه را در کنسول گوگل پلی خواهد داد و صرفا دارا بودن این کلید منجر به اعطای اجازه ی بروزرسانی، نخواهد شد .

برای ارسال برنامه به کنسول گوگل پلی 2 روش وجود دارد :

- **ارسال برنامه از طریق نسخه ی :APK** این روش به عنوان روش مرسوم جهت انتشار برنامه شناخته می شود .
- **ارسال برنامه از طریق نسخه ی :Bundle** روش جدیدی که در نسخه های اخیر اندروید استودیو اضافه شده است و برنامه را به فرمت جدید برای ارائه به کنسول گوگل پلی، آماده سازی می کند.

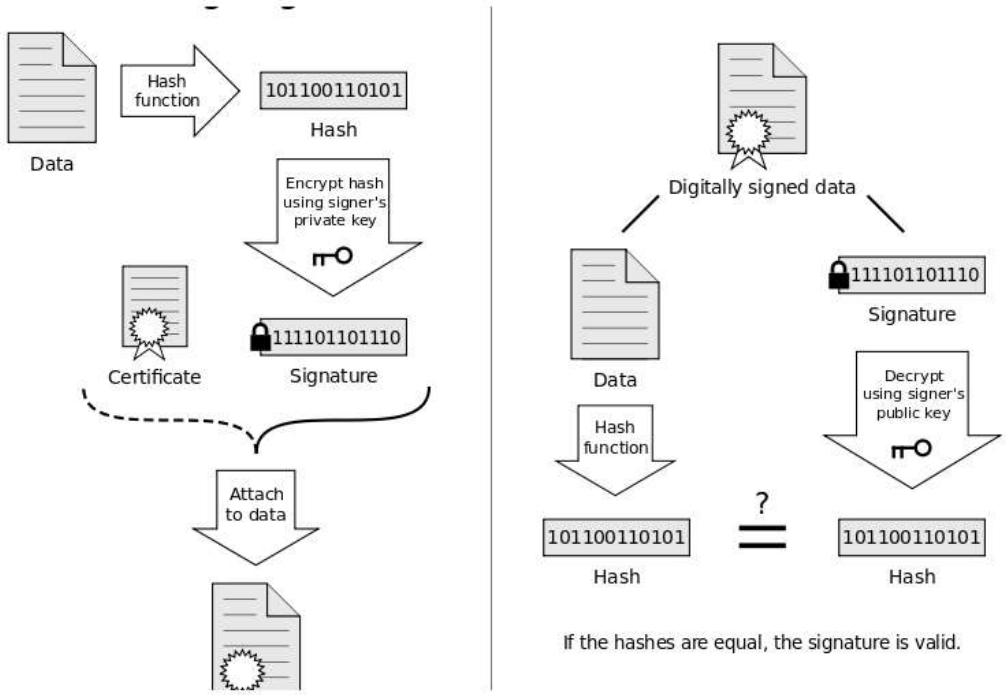
چنانچه بخواهید برنامه ی خود را از طریق روش Bundle به گوگل پلی معرفی کنید، امضا کردن برنامه به روش جدید **اجبار** است .زیرا شما Bundle برنامه خود را آپلود کرده اید و گوگل پلی نیاز دارد طی فرایندی APKبرنامه شما را قبل از انتشار تولید و سپس امضا کند. بنابراین زمانی که کلید ها توسط توسعه دهنده مدیریت شوند، راهی برای انجام دادن این فرایند توسط کنسول گوگل پلی وجود ندارد .

نکات مهم:

- اگر بخواهید نسخه امضا شده ی برنامه خود را قبل از آپلود در گوگل پلی تست کنید، شما احتمالا باید ابتدا یکبار برنامه خود را با روش سابق امضا کنید و بعد از انجام تست، نیاز دارید از طریق Upload Key، برنامه ی خود را امضا کنید و به کنسول گوگل پلی معرفی کنید.
- چنانچه برنامه خود را با روش جدید به کنسول گوگل پلی معرفی کردید، امکان بازگشت به روش قبلی وجود ندارد .
- اگر پس از انتشار برنامه توسط روش جدید، کلید Upload Key مفقود شد، میبایست ابتدا کلید Upload Keyجدید را ساخته و از طریق این صفحه از گوگل درخواست کنید تا کلید جدید را جایگزین کند.توجه کنید که شما می بایست با اطلاعات اکانت جیمیل مربوط به کنسول گوگل پلی خود این درخواست را صادر کنید.
- کلید Upload Key که توسط شما به گوگل معرفی می شود، قبل از منتشر شدن برنامه به طور کلی از برنامه شما **حذف** می شود و کلید اصلی (App Signing Key) جایگزین می شود.

جمع بندی

در این مقاله روش های امضا کردن و معرفی به کنسول گوگل پلی برای برنامه های اندرویدی گفته شد. بزرگترین مزیت استفاده از روش جدید امضا کردن برنامه که توسط گوگل پلی اخیرا معرفی شده است، **امنیت بیشتر** در برابر مفقود شدن یا ربابیده شدن کلید امضای برنامه (Keystore)است. روشی که با اجرای آن میتوانیم با خیالی آسوده امضا کردن برنامه های خود را به گوگل پلی واگذار کنیم.



منابع:

i. https://www.zoomit.ir/mobile-learning/363296-android-app-permissions/
ii. https://esaj.ir/blog/android-permissions/
iii. https://android-development.blog.ir/1393/03/02/%D8%AF%D8%B3%D8%AA%D8%B1%D8%B3%DB%8C-%D9%87%D8%A7-%D9%88-%D9%85%D8%AC%D9%88%D8%B2%D9%87%D8%A7-%D8%AF%D8%B1-%D8%A7%D9%86%D8%AF%D8%B1%D9%88%DB%8C%D8%AF
iv. https://stackoverflow.com/questions/17222535/create-system-application
v. https://virgool.io/@mpezeshkzade/googleplay-app-sign-methods-wy0xlcohawgr
vi. https://boundarydevices.com/android-security-part-1-application-signatures-permissions/
vii. https://rdzhou.github.io/2017/12/20/How-to-Sign-Android-App-with-System-Signature/

پایان.