شناسایی و تحلیل آسیب پذیری های کاربردهای اندروید با تحلیل ارتباط بین مولفه ها (ICC)

آزاده سرو عظیمی*، دانشجوی کارشناسی ارشد مهندسی نرم افزار کامپیوتر، گروه مهندسی کامپیوتر، دانشکده مهندسی، دانشگاه بوعلی سینا، همدان

a.sarveazimi@eng.basu.ac.ir

استاد راهنما : دکتر مهدی سخایی نیا، استادیارگروه مهندسی کامپیوتر، دانشکده مهندسی، دانشگاه بوعلی سینا

پاییز ۱۳۹۷

چکیده:

سیستم‌عامل اندروید یکی از پر استفاده‌ترین سیستم‌عامل‌های تلفن همراه امروزه است[۴].از آنجایی که اندروید منبع باز است، سریعترین رشد را در بین سیستم عامل‌های تلفن همراه دارد[۱].با توجه به اینکه دستگاه‌های هوشمند پایگاه کاربری بزرگی دارند و بیشتر از لپ‌تاپ-ها و دسکتاپ‌ها برای ذخیره اطلاعات شخصی حساس استفاده می‌شوند، خطر آسیب پذیری امنیتی در این دستگاه‌ها بسیار زیاد است و حفظ حریم خصوصی و امنیت کاربران گوشی‌های هوشمند به یک نگرانی بزرگ تبدیل شده است[۱].برای حفظ امنیت در معماری فعلی اندروید, لازم است هر برنامه‌ای که بر روی گوشی نصب شده و اطلاعات محرمانه کاربر بر روی آن ذخیره شده است، تحلیل شود و آسیب پذیری‌های آن شناسایی شود[۲].در سیستم‌عامل اندروید هر برنامه در یک Sandbox اختصاصی اجرا می‌شود،به همین دلیل میان‌افزار اندروید، ICC را بین اجزای برنامه واسطه می‌کند و به این ترتیب برنامه‌های مخرب به راحتی می‌توانند ارتباط بین مولفه‌های اندروید (ICC) را بکار ببرند تا به طور ناگهانی به اثرات نامطلوب دست یابند[۶]. تحلیل ICC میتواند به ما برای یافتن مشکلات امنیتی که حاصل تعاملات بین مولفه‌های مختلف یک برنامه یا چند برنامه مختلف است کمک کند[۲].

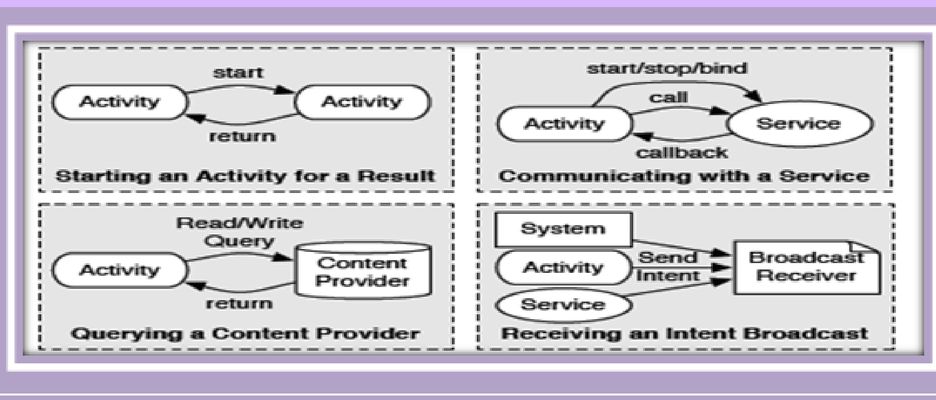
واژه‌های کلیدی: اندروید,امنیت سیستم عامل اندروید, تشخیص آسیب پذیری, بدافزار , vulnerable app, security vetting, information leakage,ICC , Privacy

۱. مقدمه:

در صنعت سیستم‌عامل گوشی‌های هوشمند , اندروید بزرگترین سهم بازار را در سراسر جهان و تعداد کاربران دارد و از طرفی با توجه به تعداد رو به رشد کاربران اندرویدی و ماهیت منبع باز این بستر,نیز مهاجمان تشویق شده اند تا دستگاه‌های اندروید را مورد هدف قرار دهند .در حالی که اندروید، برای حفاظت از دستگاه و منابع ,دارای مجوز است اما چارچوب امنیتی را برای دفاع از هر گونه حمله فراهم نمی‌کند و مهاجمان با توسعه برنامه‌های مخرب می‌توانند منجر به سرقت اطلاعات خصوصی کاربر یا استفاده ناکارآمد از منابع موبایل شوند و انواع مختلفی از مسائل امنیتی در بستر اندروید را از قبیل نشت اطلاعات، تشدید مجوز،تزریق کد مخرب، colluding و حمله‌های انکار سرویس(Dos) ایجاد کنند[۱].با درک این نواقص در معماری فعلی اندروید, لازم است هر برنامه‌ای که بر روی گوشی نصب شده و اطلاعات محرمانه کاربر بر روی آن ذخیره شده است، تحلیل شود و آسیب پذیری‌های آن شناسایی شود[۲].

۲. مفاهیم پایه:

هر برنامه در یک Sandbox اختصاصی اجرا می‌شودsandboxکردن برنامه کاربردی که همچنین به عنوان containerization برنامه کاربردی نامیده می‌شود، یک رویکردی برای توسعه نرم افزار و مدیریت برنامه‌های کاربردی موبایل (MAM) است که محیط‌هایی را که در آن برخی کدها می‌توانند اجرا شوند را محدود می‌کند[۱].در واقع Sandbox یک مکانیسم امنیتی برای جداسازی برنامه‌های در حال اجرا و محدود کردن منابع دستگاه برای برنامه است که به کمک آن دسترسی محدودی به منابع دستگاه داده می‌شود. با کمک Sandboxing برنامه فقط به منابعی از دستگاه که مجوزش اعطا شده دسترسی پیدا می‌کند[۲]. به دلیل وجود sandboxing اندروید امکان استفاده گسترده از ارتباطات بین مولفه‌ها (ICC) را ایجاد میکند که این مکانیسم برای کاهش بار مسئولیت توسعه دهندگان و ارتقاء قابلیت استفاده مجدد طراحی شده است[۳].با تحلیل ICC برنامه‌های اندروید جریان کنترلی بین مولفه ها و جریان داده‌ای بین مولفه‌های برنامه استخراج می‌گردد و آسیب‌پذیری موجود در کد برنامه و منابع موجودی که مورد سو استفاده قرار گرفته اند جستجو می‌گردد سپس بر اساس تهدیدات و آسیب‌پذیری‌های کشف شده، تصمیمی برای خرابی‌ها یا آسیب‌پذیری برنامه‌ها گرفته می-شود[۱].



شکل ۱ : ارتباط بین مولفه های برنامه

۳. کارهای مرتبط:

با توجه به تهدیدات امنیتی،تا کنون ابزارهای تحلیل بسیاری در رابطه با شناسایی آسیب-پذیری‌ها از طریق تحلیل , ICC پیشنهاد شده‌اند که تنها به بیان چند نمونه اکتفا می‌گردد:

Steven Arzt و همکاران Flowdroid را طراحی کردند که اولین راه‌حلی است که به طور کامل محتوا، شی و جریان‌های حساس را تحلیل می‌کند[۵]. این بایت کد برنامه و پیکربندی فایل‌ها را تحلیل می‌کند تا نشت‌ها را پیدا کند. Flowdroid برای شناسایی داده‌های از دست رفته ناشی از بی‌دقتی یا مورد اهداف مخرب استفاده می‌شود اما مسئله اصلی FlowDroid این است که در تجزیه دقیق و پیگیری intent , شامل تحلیل رشته پیچیده و عملیات مدیریت لیست شکست می‌خورد.

FENGGUO WEI و همکاران ابزار Amandroid را توسعه دادند که از FlowDroid الهام می‌گیرد و مدل Flowdroid را با گرفتن کنترل و وابستگی داده‌ها در میان اجزا گسترش می‌دهد[۶]. جریان Amandroid شامل تبدیل بایت کدهای دالویک برنامه‌ها به نمایش میانی، تولید مدل محیطی، ایجاد جریان داده‌ای بین مولفه ای (IDFG)، ایجاد نمودار وابستگی به داده‌ها (DDG) و سپس تشخیص امنیت است.Amandroid را می‌توان برای تشخیص نشت اطلاعات، تشخیص تزریق اطلاعات و سوء استفاده APIاستفاده کرد اما دارای یک چالشی است که برای استخراج یک گراف از بخش قابل توجهی از نمونه ها به دلیل اشکالات مجزا در کلاس‌های داخلی شکست می‌خورد و در حال حاضر Java reflection ، Dynamic class loading و فراخوانی متدهای بومی را مدیریت نمی‌کند.

۴. روش پیشنهادی و ارزیابی:

به دلیل اینکه برنامه‌های کاربردی در اندروید از طریق مکانیزم ICC با یکدیگر تعامل دارند برنامه‌ها می‌توانند مولفه‌ها یا سرویس‌های برنامه‌های دیگر را به عنوان سرویس فراخوانی کنند[۱] و از طرفی بسیاری از تهدیدات موجود در گوشی‌های هوشمند، نتیجه تعاملات بین مولفه‌های برنامه (ICC) هستند.برای شناسایی این تهدیدات امنیتی، یک تحلیل‌گر باید از جریان کنترل و جریان داده در سراسر مرزهای مولفه‌ها آگاهی داشته باشد و از طریق مکانیسم ICC می‌تواند نمودار جریان کنترل بین مولفه ها و نمودار جریان داده بین مولفه ها را استخراج کرده و از آن برای یافتن مشکلات امنیتی که حاصل تعاملات بین مولفه‌های مختلف یک برنامه یا چند برنامه مختلف است استفاده کند و به دنبال آن از طریق اطلاعات به دست آمده آسیب‌پذیری‌های کاربردهای اندروید را تحلیل و شناسایی کند[۷].

۵. نتیجه‌گیری:

تحلیل ارتباط بین مولفه‌های یک برنامه یا چند برنامه می‌تواند برای تحلیل و شناسایی آسیب-پذیری کاربردهای اندروید مورد استفاده قرار گیرد.در حال حاضر چندین تکنیک برای تحلیل ICC وجود دارند که آسیب‌پذیری‌هایی مانند نشت اطلاعات, تزریق اطلاعات و سواستفاده از API را تشخیص می‌دهند اما هر یک دارای چالش‌هایی هستند و یا برای تعداد زیادی از برنامه‌های کاربردی مقیاس پذیر نیستند[۸].علاوه بر اینکه تحلیل ICC می‌تواند برای تحلیل و شناسایی آسیب‌پذیری‌های کاربردهای اندروید استفاده شود می‌تواند برای رفع انواع آسیب-پذیری نیز استفاده گردد[۸].

۶. منابع:

[۱]Bahman Rashidi, Carol Fung.2015. A Survey of Android Security Threats and Defenses

[۲] Damien Octeau,Patrick McDaniel, Somesh Jha, Eric Bodden, Jacques Klein,Yves Le Traon.2013. Effective Inter-Component Communication Mapping in Android with *Epicc*:An Essential Step Towards Holistic Security Analysis

[۳] Fred Guyton .2018.A survey of Android security threats and machine learning techniques used for detection.

[۴] Jamil Khan.2015. Android Architecture and Related Security Risks

[۵]i Li, Alexandre Bartel, Tegawendé F Bissyandé, Jacques Klein, Yves Le Traon,Steven Arzt, Siegfried Rasthofer, Eric Bodden, Damien Octeau, and Patrick Mc-Daniel. 2015. IccTA: Detecting Inter-component Privacy Leaks in Android Apps. In Proc. of ICSE'15.

[۶] FengguoWei, Sankardas Roy, Xinming Ou, and Robby. 2017. Amandroid: A Precise and General Inter-component Data Flow Analysis Framework for Security Vetting of Android Apps. Technical Report 2017-4. University of South Florida, USA.

[۷] Keyur Kulkarni, Ahmad Y Javaid.2018. Open Source Android Vulnerability Detection Tools: A SurveyApplication Certification

[۸] Damien Octeau ,Patrick McDaniel,Somesh Jha,Eric Bodden,Jacques Klein , Yves LeTraon. 2013.Effective Inter-Component Communication Mapping in Android with *Epicc*