بسمه تعالی

مرکز تخصصی آپا دانشگاه رازی گزارش می‌دهد

مرکز تخصصی آپا دانشگاه رازی

" چند توصیه امنیتی به برنامه نویسان برنامه های کاربردی سیستم عامل آندروید"

نسخه‌ی کامل خبر

آرمان محمودی

۸ مرداد ۱۳۹۶

چگونه امنیت برنامه های کاربردی را بیشتر کنیم؟

سیستم عامل آندروید راه های گوناگونی برای ایجاد امنیت برنامه های کاربردی خود دارد به عنوان مثال برنامه ی سندباکس، حفاظت در برابر بافر و حملات سرریز عدد صحیح از قابلیت امنیتی سیستم های عامل آندروید است .به عنوان یک نتیجه یک برنامه ی ساده آندروید که به هیچ کدام از فایل‌های شخصی کاربر ندارد یا دسترسی برنامه کاربردی به شبکه های محلی WIFI شبکه اینترنت دارای محدودیت است ، دارای سطح امنیتی در حالت پیش فرض می‌باشد .

با رعایت چند اصل ساده می‌توان سطح امنیت برنامه های کاربردی در سیستم عامل آندروید را افزایش داد . این اصول در حین توسعه دادن برنامه کاربردی به کار می‌روند و برای توسعه دهندگان برنامه‌های کاربردی سیستم عامل آندروید در نظر گرفته شده است:

1. استفاده از حافظه داخلی هر برنامه کاربردی برای داده‌های حساس
2. رمز نگاری داده‌هایی که در حافظه‌ی خارجی ذخیره می‌شوند
3. استفاده از Intent برای تبادل و ارتباط بین پردازشی (IPC)
4. استفاده از HTTPS در برنامه‌هایی که به صورت آنلاین به روز رسانی می‌شوند
5. جایگزین کردن GCM با سرویس پیام رسانی (SMS)
6. اجتناب کردن از پرسیدن اطلاعات شخصی کاربر
7. تایید ورودی کاربر

1. استفاده از حافظه داخلی هر برنامه کاربردی برای داده های حساس

در سیستم عامل آندروید حافظه‌ی دستگاهی که عرضه می‌شود به دو قسمت تقسیم می‌گردد:

حافظه داخلی و حافظه دستگاه

بیشتر برنامه های کاربردی که توسعه داده می‌شوند به مقداری حافظه برای ذخیره سازی اطلاعات برنامه مورد نظر نیاز خواهند داشت. از طرف دیگر هر برنامه کاربردی در سیستم عامل آندروید دارای مقداری حافظه مشخص در حافظه داخلی می‌باشد .

این حافظه بسته به دستگاهی که برنامه بر روی آن نصب می‌شود و یا با نظر برنامه نویس می‌تواند تعیین شود. این قسمت از حافظه برای هر برنامه کاربردی دارای سطح امنیتی بوده و کاربر نمی‌تواند به محتوای آن دسترسی داشته باشد یا به اصطلاح در حالت private-mode قرار دارد. برنامه های کاربردی نصب شده روی دستگاه هم به این قسمت از حافظه دسترسی ندارند. به همین علت بهترین مکان برای ذخیره‌سازی اطلاعات حساس در این قسمت از حافظه می‌باشد.

ولی سیستم عامل یک مقدار محدود از این حافظه را در اختیار برنامه نصب شده قرار می‌دهد . از این رو در ابتدای برنامه نویسی باید فایل های حساس را شناسایی کرد.

2. رمز نگاری داده‌هایی که در حافظه ی خارجی ذخیره میشوند

ظرفیت حافظه داخلی برای هر برنامه کاربردی محدود بوده و نمی‌توان که کل حافظه داخلی را در اختیار یک برنامه کاربردی خاص گذاشت . از طرف دیگر برنامه هایی وجود دارند که به حافظه‌ی بیشتری نیاز خواهند داشت. لذا توسعه دهنده برای ذخیره سازی اطلاعات برنامه هایی که حافظه بیشتری نسبت به حافظه داخلی نیاز دارند چاره ای به جز استفاده کردن از حافظه‌ی خارجی ندارد. حافظه خارجی به کل حافظه‌ی که دستگاه در اختیار دارد گفته می‌شود میتواند حافظه‌ی خود دستگاه یا یک کارت حافظه باشد. ولی زمانی که برنامه نویس از این فضا استفاده می‌کند همه‌ی برنامه های کاربردی نصب شده روی دستگاه و کاربر می‌تواند به آن دسترسی داشته باشند. به همین علت دارای سطح امنیتی پایین می‌باشد . راه‌حل این است که برنامه نویس داده‌ها و اطلاعاتی که در حافظه خارجی ذخیره می‌کند به صورت رمزنگاری شده باشد. یکی از مشهورترین

الگوریتم‌های رمزنگاری که در برنامه‌نویسی آندروید از آن استفاده می‌شود AES مخفف Advanced Encryption Standard با اندازه کلید ۲۵۶ بیتی می‌باشد .

Partition	Explanation
/boot	kernel & Co.
/cache	app cache
/data	user data partition
/data/data	app data
/dev	devices
/mnt/asec	encrypted apps (App2SD)
/mnt/emmc	internal sdcard
/mnt/sdcard	external sdcard
/proc	process information
/recovery	used in recovery mode
/system	system ROM (read-only)

جدول ۱: پوشه های مهم سیستم عامل آندروید برا ذخیره سازی داده ها

3. استفاده از Intent برای تبادل و ارتباط بین پردازشی (IPC)

برای تبادل اطلاعات و ارتباط درون برنامه‌ای در سیستم عامل آندروید راه‌های زیادی وجود دارد برای مثال استفاده از سوکت ، names pips و یا اشتراک‌گذاری فایل‌ها . این روش‌ها معمولا مستعد تهدید می‌باشند .

برای مثال برنامه‌ی کاربردی

برای ایجاد ارتباط درون برنامه‌ای و تبادل اطلاعات بین برنامه‌ای نصب شده در سیستم عامل آندروید راه‌حل بهتری نیز وجود دارد استفاده کردن از Intent ها. این راه‌حل هم دارای سطح امنیتی بالاتری نسبی به روش‌های گفته شده دارد و هم استفاده کردن از ان بسیار آسان است. Intent ها به برنامه نویس این اجازه

می‌دهند که اطلاعات لازم را برای برنامه‌های کاربردی نصب شده روی دستگاه بفرستد و برنامه مقصد اطلاعات را دریافت کند و بر اساس آن اجرا شود.

4. استفاده از HTTPS در برنامه هایی که به صورت آنلاین به روز رسانی میشوند

امروزه استفاده کردن از برنامه‌هایی که بتوان به صورت خودکار به روز رسانی شوند بسیار مرسوم است. این برنامه ها معمولا به یک سرویس دهنده متصل شده و اطلاعات جدید را از سرویس دهنده مورد نظر دریافت می‌کنند. برای ایجاد ارتباطی امن بین دریافت کننده اطلاعات و سرویس دهنده بهتر است از ارتباط HTTPS استفاده شود.

5. جایگزین کردن GCM با سرویس پیام رسانی (SMS)

قبل از پیدایش GCM (Google Cloud Messaging) توسط گوگل معمولا برای ایجاد ارتباط بین سرویس‌دهنده و سرویس‌گیرنده از سیستم پیام‌رسانی استفاده می‌کردند. ولی در سیستم عامل آندروید دسترسی به پیام‌ها و سیستم پیام‌رسانی بسیار ساده می‌باشد و با یک اجازه نامه در فایل manifest می‌توان به آن‌ها دسترسی داشت لذا برای بالا بردن اطمینان و امنیت برنامه‌های کاربردی می‌توان از سرویس پیام‌رسان ابری گوگل استفاده کرد. این سرویس پیام رسانی دارای ضریب امنیتی بالا می‌باشد .

GCM دارای ویژگی‌های زیر است:

- این امکان را به برنامه‌های تحت وب می‌دهد که پیام‌های خود را برای برنامه‌های سیستم عامل آندروید بفرستند. برای راه اندازی این سرویس باید یک ارتباط مستقیم بین برنامه‌ی کاربردی سیستم عامل آندروید و برنامه کاربردی وب ایجاد شود.
- برای دریافت پیام‌ها در گوشی‌های همراه به دریافت کننده‌ی پیام نیاز نیست

- این سرویس انعطاف‌پذیر است و برنامه کاربردی به صورت دلخواه می‌تواند از آن استفاده کند به عنوان مثال می‌تواند از اعلان‌ها ، پیام‌ها برای نمایش این سرویس استفاده کند.
- این سرویس برای نسخه های آندروید ۲٫۲ در دسترس است

6. اجتناب کردن از پرسیدن اطلاعات شخصی کاربر

امروزه اطلاعات شخصی کاربران دارای اهمیت ویژه ای می‌باشد به طوری که قانون‌هایی مانند دستورالعمل حفاظت از اطلاعات اتحادیه اروپا و قانون حفاظت از اطلاعات شخصی و اسناد الکترونیکی کانادا، استفاده از اطلاعات کاربران را ممنوع کرده است. بنابراین تا یک زیرساخت امن برای جمع آوری و ذخیره سازی اطلاعات برای کاربران وجود نداشته باشد نمی‌توان در برنامه کاربردی به طور مستقیم از کاربران درخواست اطلاعات شخصی کنید .

یک راه‌حل امن برای تایید هویت کاربر و تکمیل اطلاعات شخصی کاربر در پروفایل شخصی استفاده از Google Identity Platform پلتفرم تایید هویت گوگل است تا با استفاده از حساب کاربری گوگل وارد برنامه‌های کاربردی شوند. بعد از ورود به برنامه از طریق حساب کاربری گوگل برنامه کاربردی می‌تواند اطلاعات شخصی مانند عکس پروفایل، نام کاربری و... را از کاربر بپرسد و آن را ذخیره کند. این بستر دارای تایید امنیت گوگل می‌باشد.

7. تایید ورودی کاربر

در سیستم عامل آندروید معمولا داده های نامعتبر موجب ایجاد مسائل امنیتی مانند سرریز شدن بافر نمی‌شود ولی با این حال اگر برنامه کاربردی به یک پایگاه داده یا یک سیستم ارائه دهنده محتوا متصل باشد،

باید ورودی‌هایی که کاربر وارد می‌کند بررسی شود. عدم این بررسی‌ها می‌تواند باعث ایجاد حمله‌ی SQL Injection شود.

منابع:

1- “Ahmed Mohamed Gamaleldin ” -How To Develop Smart Android Notifications using Google Cloud Messaging Service-2013
2- “William Enck, Machigar Ongtang, and Patrick McDaniel” -Understanding Android Security -2012