پایان نامه دوره کارشناسی مهندسی فناوری اطلاعات

گرایش فناوری اطلاعات

موضوع:

سیستم عامل اندروید و امنیت آن

استاد راهنما:

نگارش:

خرداد 1394



پایان نامه دوره کارشناسی مهندسی فناوری اطلاعات

گرایش فناوری اطلاعات

موضوع:

سیستم عامل اندروید و امنیت آن

استاد راهنما:

نگارش:

خرداد 1394

وزارت علوم ,تحقیقات و فناوری

دانشگاه جامع علمی- کاربردی

مرکز آموزش علمی – کاربردی قوچان

گزارش پروژه کاردانی/کارشناسی رشته ............................

عنوان پروژه...........................

در تاریخ .........................توسط استاد راهنما ،پروژه دانشجو .............................به شماره

دانشجویی ....................................بررسی و با نمره به عدد ............... به حروف ...................به تصویب نهایی رسید.

نام استاد راهنماي پروژه امضاء و تاریخ

امضاء مدیر گروه

من لم يشکر المخلوق لم يشکر الخالق

تقدیر و تشکر

سپاس و ستايش ويژه خدا است ، خدائى كه با نيروى قلم ، انسان را با علم و دانش آشنا ساخت ، علم و دانشى كه بشر با آن ، سابقه و آشنائى نداشت.

شکر خداوند متعال را به جاي آورده که توفيق نصيب ما کرد تا اين پروژه را به پايان برسانیم.

با سپاس فراوان

# چکیده :

اندروید یک پلتفرم موبایل مدرن و هوشمند است که بصورت آزاد انتشار یافته است. البته خبرهایی از اینکه احتمال دارد گوگل به یکباره اندروید را تجاری کند نیز بگوش میرسد. اپلیکیشن های اندرویدی از نرم افزار و سخت افزار حرفه ای استفاده میکنند. و نیز از پشتیبانی شرکتی و مردمی بهره می برد که ارزشهایی برای مصرف کننده دارد. برای حفاظت از این ارزش ها پلتفرم باید محیط برنامه ای رو ارائه بده که امنیت کاربران، اطلاعات، برنامه ها، دستگاها و شبکه ها را تامین کند. لازمه امن کردن پلتفرم باز معماری امنیتی قدرتمند و برنامه های امن دقیق میباشد. اندروید طراحی شده با امنیت چند لایه ای که انعطاف پذیری لازم برای پلتفرم باز را فراهم میکند.

در فصل اول با نگاهی کلی به انواع سیستم عامل موجود سعی بر معرفی انواع سیستم عامل نموده ایم ،در فصل دوم تلاش بر شناساندن تاریخچه و ورژن های متفاوت سیستم عامل اندروید و به تفهیم واژه اندروید هستیم و در نهایت در فصل آخر با بیان امنیت در اندروید پرداخته ایم.

بدین ترتبت نتیجه میگیریم که سیستم عامل اندروید یکی از معرف ترین و کارآمد ترین سیستم عامل های موجود در جهان می باشد که از زمان پیداش تاکنون علی رغم نقاط قوت و و ضعف در ویرایش های مختلف آن،همواره در مسیر تکاملی خود سعی بر کاهش نقاط ضعف و رسیدن به امکانات و خدمات مطلوب کاربران کرده است.

کلمات کلیدی : پلتفرم - اپلیکیشن - موبایل - ورژن - سیستم عامل – اندروید – امنیت

فهرست مطالب

[چکیده : ح‌](#_Toc423437642)

[فصل اول](#_Toc423437643) [نگاهی کلی به انواع سیستم عامل های موجود در جهان 1](#_Toc423437644)

[مقدمه 2](#_Toc423437645)

[1 - انواع سیستم عامل ها 3](#_Toc423437646)

[1 – 1 اندروید 4](#_Toc423437647)

[1– 2 سیستم عامل iphone 5](#_Toc423437648)

[1 – 3 سیستم عامل (osx ) 6](#_Toc423437649)

[1 – 4 سیستم عامل سیمبین 6](#_Toc423437650)

[1 – 5 سیستم عامل بلک بری 7](#_Toc423437651)

[1 – 6 وینوز فون 7 8](#_Toc423437652)

[1 -7 سیستم عامل لینوکس (LINUX) 9](#_Toc423437653)

[فصل دوم](#_Toc423437654) [سیستم عامل اندروید 13](#_Toc423437655)

[مقدمه 14](#_Toc423437656)

[2-1 تاریخ مختصر اندروید 14](#_Toc423437657)

[2-2 معنای اندروید 15](#_Toc423437658)

[2-3 تولد یک آدم آهنی! 15](#_Toc423437659)

[2-4 آدم آهنی تقویت می شود 16](#_Toc423437660)

[2-5 کپی رایت و حق امتیاز 17](#_Toc423437661)

[2-6 توضیح انواع مدل های اندروید 17](#_Toc423437662)

[2-6-1 نسخه 1 و2 17](#_Toc423437663)

[2-6-2 نسخه 1،5-CUPCAKE 17](#_Toc423437664)

[2-6-3 نسخه 6و1 –DONUT 18](#_Toc423437665)

[2-6-4 نسخه 2 و 1،2 19](#_Toc423437666)

2-6-5[FROYO نسخه 2،2 20](#_Toc423437667)

2-6-6[GINGERBREAD نسخه 2،3 20](#_Toc423437668)

2-6-7 [Honeycomb نسخه 3 و3،1 و3،2 22](#_Toc423437669)

2-6-8[Ice Cream Sandwich نسخه 4 22](#_Toc423437670)

[2-7 میزان محبوبیت نسخه های مختلف اندروید 24](#_Toc423437671)

[2-8 سرعت انتشار ویرایش های اندروید فرصت ها وتهدید ها 24](#_Toc423437672)

[2-9 سهم بازار اندروید 25](#_Toc423437673)

[2-10 دستگاه های شاخص مبتنی بر اندروید 27](#_Toc423437674)

[2-11 اندروید مارکت 28](#_Toc423437675)

[2-12 تم انحصاری سازندگان 31](#_Toc423437676)

[2-13 رابط کاربری صفحات خانگی 32](#_Toc423437677)

[2-14 آیکن ها 32](#_Toc423437678)

[2-15 پوشه ها 33](#_Toc423437679)

[2-16 ویجتها 33](#_Toc423437680)

[2-17 فواید اجرا کننده های اختصاصی 34](#_Toc423437681)

[2-18 لذت چند رسانه ای و مدیریت 35](#_Toc423437682)

[2-19 استریم مدیا 36](#_Toc423437683)

[2-20 دست دوستی با ITUNES 37](#_Toc423437684)

[2-21 بازارچه اندروید 38](#_Toc423437685)

[2-22 نرم افزار هدایت گر و به روز رسانی ها 39](#_Toc423437686)

[2-23 روت کردن اندروید 40](#_Toc423437687)

[2-24 چگونه روت کنیم 41](#_Toc423437688)

[2-25 نصب نرم افزارهایی که در مارکت نیستند 41](#_Toc423437689)

[2-26 شخصی سازی آهنگ های زنگ و پیام 43](#_Toc423437690)

[2-27 امنیت و اهمیت دسترسی ها 43](#_Toc423437691)

[2-28 ابراز مبارزه با MALWARE ها – دفاع غیر عامل 44](#_Toc423437692)

[2-29 مانیتورینگ گوشی 45](#_Toc423437693)

[2-30 امنیت فیزیکی 46](#_Toc423437694)

[2-31 دلایل برتری گوشی های اندروید در مقایسه با آیفون 46](#_Toc423437695)

[2-32 آینده اندروید 49](#_Toc423437697)

[2-33 اندروید و گوگل تی وی 49](#_Toc423437698)

[فصل سوم](#_Toc423437699) [امنیت در اندروید 50](#_Toc423437700)

[مقدمه 51](#_Toc423437701)

[3-1 دیکامپایلر ded 57](#_Toc423437704)

[3-2 بازگردانی برنامه 58](#_Toc423437705)

[3-3 بهینه سازی و دیکامپایل کردن 62](#_Toc423437707)

[3-4 اعتبار سنجی بازیابی سورس کد 64](#_Toc423437709)

[3-5 ارزیابی امنیت اندروید 66](#_Toc423437710)

[3-6 ویژگی های تجزیه و تحلیل 66](#_Toc423437711)

[3-7 نتایج تحلیلی برنامه ها 69](#_Toc423437713)

[3-8 برنامه های کاربردی نصب شده 81](#_Toc423437716)

[3-9 حملات تزریقی مقصد 86](#_Toc423437718)

[3-10 کار مرتبط با امنیت 88](#_Toc423437719)

[3-11 مرور برنامه ی امنیتی اندروید 90](#_Toc423437720)

[3-12 بازنگری طراحی 90](#_Toc423437721)

[3-13 تست نفوذپذیری و بازنگری کدها 91](#_Toc423437722)

[3-14 بازنگری Opensource و انجمنها 91](#_Toc423437723)

[3-15 واکنش به مشکلات 91](#_Toc423437724)

[3-16 معماری امنیتی پلتفرم اندروید 91](#_Toc423437725)

[3-17 امنیت سطح کرنل و سیستم 93](#_Toc423437727)

[3-18 توصیه هایی برای امنیت بیشتر اندروید 94](#_Toc423437728)

[3-19  انواع برنامه های خطرناک 94](#_Toc423437729)

[3-20 چگونه بدافزارها به دستگاه های اندرویدی راه پیدا می کنند 100](#_Toc423437730)

[3-21  ترفندهای ساده برای محافظت از امنیت موبایل 101](#_Toc423437731)

[3-22 پیشنهاد برای استفاده از ضد بدافزار 102](#_Toc423437732)

[3-23 امنیت اندروید را جدی بگیرید 103](#_Toc423437733)

[3-24 اندروید، قدرت نفوذ بدافزارها را کاهش می دهد 107](#_Toc423437734)

[3-25 هک کردن گوشی های اندروید 107](#_Toc423437735)

[3-26 روت کردن چیست؟ 107](#_Toc423437736)

[3-27 چرا گوشی را Root کنیم؟ 108](#_Toc423437737)

[3-28 اپلیکیشن های ارزشمند و مهم 109](#_Toc423437738)

[3-29 راه هایی برای محافظت از دستگاه اندرویدی در برابر ویروس 109](#_Toc423437739)

[فصل چهارم](#_Toc423437740) [نتیجه گیری 115](#_Toc423437741)

[منابع 118](#_Toc423437742)

فهرست اشکال و جداول

[شکل 2- 1 مقایسه آیفون و اندروید 47](#_Toc423437375)

[شکل 3- 1معماری سیستم اندروید 54](#_Toc423437381)

[شکل 3- 2 فرایند کامپایل برنامه های DVM 55](#_Toc423437382)

[شکل 3- 3بازگردانی بایت کد دالویک 58](#_Toc423437385)

[جدول 3- 1برنامه های کاربردی مطالعه شده ( از بازار اندروید ) 64](#_Toc423437387)

[شکل 3- 4مثال ویژگی های کنترل جریان 68](#_Toc423437391)

[جدول 3- 2دستیابی به شناسه هایAPI های تلفن 70](#_Toc423437393)

[جدول 3- 3آشکارسازی جریان های داده برای سینک های شبکه 72](#_Toc423437394)

[شکل 3- 5استراق سمع در مفاهیم محافظت نشده 85](#_Toc423437396)

# فصل اول

# نگاهی کلی به انواع سیستم عامل های موجود در جهان

# مقدمه

پایان نامه پیش رو در رابطه با سیستم عامل موبایل اندروید می باشد که مشتمل بر سه فصل خواهد بود.در فصل اول با نگاهی کلی به انواع سیستم عامل موجود سعی بر معرفی انواع سیستم عامل نموده ایم ،در فصل دوم تلاش بر شناساندن تاریخچه و ورژن های متفاوت سیستم عامل اندروید و به تفهیم واژه اندروید هستیم و در نهایت در فصل آخر با بیان امنیت در اندروید پرداخته ایم.

تلفن های همراه هوشمند در سال های اخیر به برکت توسعه سیستم عامل های بر پایه سکوهای موبایل ،توسعه شگرفی یافته اند.به همین منظور در گزارشی به بررسی عملکرد مهمترین سیستم عامل های موبایل که بافناوری لمس سازگاری دارند پرداخته ایم:

به گزارش پایگاه خبری فناوری اطلاعات برسام و به نقل از خبر گزاری مهر ،انقلاب موبایل که از زمان ورود آیفون در سال 2007 آغاز شد امروزه تمام بخش ها از تولید تلفن های همراه هوشمند تا سیستم عامل های صفحه لمسی و دریایی از برنامه های جانبی و نرم افزار های مفید را در بر گرفته است.

تلفن های همراه هوشمند توانسته اند یک تغییر ریشه ای در شکل ارتباطات همراه ایجاد کنند که این تغییر تمام ساختارهای اجتماعی راتحت تاثیر قرارداده است .

برای درک بهتر این تحول بیادی و جهانی بهتر است که کمی به دنیای موبایل در دو سه سال قبل توجه کنیم . امروز طیف وسیعی از گوشی های موبایل عرضه شده اند : از تلفن های همراه ارزان تا تلفن های همراه هوشمند گران با عملکرد های مختلف.

شکل دستگاها نیز نسبت به دو سال پیش تغییراتی اساسی کرده اند.سیستم های عامل های صفحه لمسی امروزه به توید کنند گان این اجازه را داده اند که رو به تولید تلفن های همراه هوشمند صفحه لمسی تمایل پیدا کنند.این سیستم عامل های مدرن و پیشرفته موفق شده اندتجربه ای جدید از ارتباطات همراه برای کاربران به ارمغان آورند و تعامل کاربر با شبکه و محتویات چند رسانه ای را بهبود بخشند .

اما تنوع روز افزون تلفن های همراه هوشمندی که ظاهری تقریبا مشابه دارندانتخاب برای کاربران دشوار شده است. به طوری که اغلب این سوال پرسیده میشود که کدام گوشی هوشمند بهتر است ؟

در اینجا برای پیدا کردن پاسخی مناسب به این سوال بسیار رایج ،تلفن های همراه هوشمند بر پایه نوع سیستم عاملی که استفاده میکنند مورد بررسی قرار می گیرند

# 1 - انواع سیستم عامل ها

* سیستم عامل سیمبینSymbian ) )
* سیستم عامل لینوکسLinux) )
* سیستم عامل بلک بریBlack berry) )
* سیستم عامل ویندوز موبایل Windows mobile) )
* سیستم عامل مک (اپل ) (Apple mac ios)
* سیستم عامل اندروید گوگلAndroid) )
* سیستم عامل باداBada ) )
* سیستم عامل میامو (Meamo)
* سیستم عمل میگو( meego)
* سیستم عامل پالمpalm) )

# 1 – 1 اندروید

نقاط قوت :تداخل ساده و واقعی، جستجوی ماهوارهای رایگان ،دسترسی راحت و سریع به جی-میل

نقاط ضعف :تلفن های همراه هوشمند مجهز به این سیسنم نمی توانند با نسخه های جدید تر بروز شوند.

اگر سیستم عامل آیفون ، شایسته عنوان ایجاد تداخل آسان با لمس است اندروید را باید به عنوان سیستم عاملی که تلفن های همراه هوشمند را دستخوش تحول کرد به رسمیت شناخت.

این سیستم عامل گوگل بدلیل انعطاف پذیری و کم مصرف بودن مورد توجه تولید کنندگان مطرح در دنیا قرار گرفته است.

امروزه اندروید بی شک سیستمی با قابلیت بیشترین رشد است. در حال حاضر بسیاری از محصولات سامسونگ ، سونی اریکسون ،موتورلا و ال جی بر پایه این سیستم عامل قرار دارند.

اندروید پس از بعضی ناپایداری های اولیه به سرعت به سمت ثبات و صحولت در استفاده شخصی رسید. بدون در نظر گرفتن این فروشگاه مجازی این سیستم عامل یکی از بزرگترین ارائه دهندگان برنامه های نرم افزار جانبی است ، تمام تلفن های همراه هوشمندی که بر پایه این سیستم عامل هستند می توانند نقشه ها و نرم افزار موقعیت یابی ماهواره ای گوگل را به صورت رایگان بارگذاری کنند. در ادامه در رابطه با این سیستم عامل بیشتر صحبت خواهیم کرد.

# 1– 2 سیستم عامل iphone

نقاط قوت :تداخل آسان لمس ،سازگار پذیری و امکان تصحیح عملکرد

نقاط ضعف : سازگاری تنها با محصولات اپل و بنابر این توسعه محدود

زمانی که نمایشگر صفحه لمسی به عنوان تنها بهانه موجود برای شگفت زده کردن دوستلن شناخته میشد،اپل دانست که باید در سیستم عامل موبایل جدید خود از این فناوری به عنوان برگ برنده استفاده کند. به این ترتیب این فناوری را مجهز به یک "تداخل جامد کنترل " کرد و به کاربر اجازه داد که با دو انگشت زوم نمایشگر را تغییر دهد.

اینگونه سیستم عاملی شکل گرفت که پیش از ان هرگز مثل ان مشاهده نشده بود . تنها رد زمان اخیر است که شکاف سیستم عامل ها ی دیگر این سکوی اپل را وارد بازار رقابت کرده است .

این سیستم عامل برای شرکت ایستو جابز نقاط ضعف و قوت بسیاری داشته است .به طوری که از یک سو این سیستم عامل " آی فن"تنها از یک تلفن همراه حمایت میکند (مدل های مختلف این تلفن همراه همگی به عنوان یک خانواده واحد شناخته میشوند) سازگار پذیری و امکان تصحیح عملکردها را آسان می کند ،اما از سوی دیگر سرنوشت این سیستم عامل اپل تنها با تلفن های همراه این شرکت گره می خورد و بنابراین محکوم به یک توسعه محدود می شود.

# 1 – 3 سیستم عامل (osx )

این سیستم عامل توسط شرکت اپل و برای استفاده بر روی آیفون طراحی وهسته اصلی آن از MAC OSX گرفته شده است

با توجه به استفاده محدود این سیستم عامل تنها در گوشی های آیفون طبیعی طبیعی است که رونق چندانی در بازار ندارد و مورد توجه کاربران نیست.سهم این سیستم عامل تنها 3/1% کل بازار است .

# 1 – 4 سیستم عامل سیمبین

* سال تاسیس این شرکت نرم افزاری :1998
* هدف از تاسیس این شرکت :کار بر روی سیستم عاملی برای کار بر روی موبایل
* مقر اصلی تاسیس این شرکت :انگلیس

نقاط قوت :ثابت و بدون شگفتی ،لزوما نباید بر پایه صفحه لمسی باشد،موقعیت یاب ماهواره ای رایگان

نقاط ضعف :فناوری لمس آن در سطح رقابت با سایر محصولات نیست. برنامه جانبی کمی بر روی فروشگاه جانبی آنلاین وجود دارد.

سیمبیان سیستم عاملی است که بیشترین رنج و آسیب را از انقلاب فناوری صفحه لمسی دید. گذر از سیمبیان سر ی60 ثابت و بسیار گسترده تا سیمبیان سری 60 ویرایش 5 متقائد کننده نبود. به همین علت نوکیا تا زمان عرضه نسخه آینده این سیستم عامل (سیمبیان سری 3) باید کاهش رقم خود را در بازار تلفنهای همراه هوشمند را تحمل کند.

ارتباط میان این سیستم عامل و تولید کنندگان فندلاندی موجب شد که یک تاخیر ملموس در تولید تلفن های همراه هوشمند این شرکت ایجاد شود.زبان اصلی برنامه نویسی برای سیمبینC++ است.

سیمبیان با این زبان نوشته شده است و معماری آن مبتنی بر پلاگین است که افزودن فناوری های مورد نظر شرکت های مختلف به آن راآسانتر می کند. این سیستم عامل ازا نواع سخت افزارهای مختلف پشتیبانی میکند (مزیتی کلیدی در بازار اسمارت فون ها) واجرای قابلیت جدید ودرخواستی را سریعتر انجام می دهد.

هر یک از این زبان ها می توانند امکانات کامل برنامه نویسی در سیمین را فراهم کنند.رشد زبان های برنامه نویسی در این سیستم عامل سریع می باشد.به طوری که نصف این زبان ها همین امسال وارد این سیستم عامل شده اند و بدون شک این رشد با ورود زبان های دیگر ادامه خواهد یافت. ابزارهای برنامه نویسی مختلفی از جمله ادیتور های متنوع نیز برای کار با این زبان ها به همراه شبیه سازی موبایل به بازار عرضه شده است

# 1 – 5 سیستم عامل بلک بری

* درژانویه 1999 نسخه ی 1.0سیستم عام Black –berryرونمایی شد
* نسخه ی 3.6 برای گوشی 5810 در مارچ 2012 عرضه شد.
* درآپریل 2010 نسخه 6.0 سیستم عاملBlack-berry رونمائی شد.
* درسپتامبر 2010 سیستم عامل Black-berry tablet os معرفی شد.
* در ماه می 2011 شرکت RIM از سیستم عامل شماره 7 بلک بری رونمایی کرد.

نقاط قوت :پست الکترونیک بدون رقیب ،فروشگاه مجازی ویژه دنیای تجارت ، تداخل آسان با سرویس های ارسال پیام

نقاط ضعف : مرورگر و چند رسانه ای ناکامل ،تداخل لمسی قابل بهبود

این سیستم عامل خوب است و همیشه با تلفن همراه هوشمندی که کابران بسیار وفاداری دارد ،جان بخشیده است

این شرکت کانادایی همیشه به دنبال مشتریانی بوده است که از این تلفن همراه هوشمند استفاده کاری میکنند و بنابراین امکانات آن را به گونه ای سازمان دهی کرده است حتی کاربرانی که توانایی و یا فرصت کافی برای استفاده از عملکردهای پیچیده و پیشرفته فناوری را ندارند نیز بتوانند به صحولت از خانواده بلک بری استفاده کنند.

در این راستا ،در عرصه چند رسانه ای نیز ،سیستم عامل بلک بری محدودیت های بسیاری دارد .

RESEARCH IN MOTION در آستانه عرضه نسخه جدیدی از سیستم عامل بلک بری با عنوان 6.0 OS قرار داردکه با نمایشگرهای

حساس به لمس سازگار است.به این ترتیب اولین مدلهای بلک بری بدون صفحه کلید در راهند.

شرکت TENDMICRO بر طبق تحقیقاتی که انجام داد اعلام نمود که سیستم عامل بلک بری 7 امن ترین سیستم عامل مورد استفاده در تلفن های همراه می باشد.

# 1 – 6 وینوز فون 7

* از سال 1996 بنیان گذاشته شد.
* توسط شرکت MICROAOFTساخته شده است.
* OPEN SORCE نیست.

نقاط قوت :تداخل لمس مدرن و کاربردی ،امکان ساماندهی بسیار خوب تماسها ،برخورداری از استاندارهای ویژه برای تلفن های همراه.

نقاط ضعف :مرورگر قابل بهبود،فروشگاه مجازی با برنامه های مجازی کم.

زمانی دستگاه ویندوز موبایل به عنوان تلفن های همراه بسیار عالی شناخته میشدند.مقام اولی که در گذر سالها رنگ وبوی خود را از دست داد و به این ترتیب مایکروسافت نیز به یکی از شرکت هایی تبدیل شد که از تکامل لمس رنج میبرد. بنابر این ویندوز فن 7 جدید با تمام نیازهای بازار لمس را تامین کند تا بتواند بار دیگر موفقیت خود را باز یابند.

به نظر میرسد شرکت ردموند تلاش خود را در این عرصه آغاز کرده است به طوری که ائتلافهای استراتژیکی را با تولید کنندگان تلفن های همراه هوشمند منعقد کرده است اما باید بر روی جنبه توسعه برنامه های جانبی تمرکز بیشتری کند.در حقیقت امروز برنامه های جانبی همانند یک اسب تراوای مهم هستند که می توانند یک سیستم عامل را در قلب کاربرانشان عزیز کنند .در این راستا ،ادغام سیستم عامل ویندوز فن 7 "با ایکس باکس لایو" علاقمندان بازی های ویدیویی را به سوی تلفنهای همراه هوشمند برپایه ویندوز فن 7 جلب کند.

# 1 -7 سیستم عامل لینوکس (LINUX)

این سیستم عامل بر اساس هسته سیستم عامل لینوکس توسعه یافته است .در واقع مدیریت و بهینه سازی حافظه ،ارتباط با سخت افزار وسرویس های سیستم ،امنیت ،مدیریت پردازش ها و مدیریت منابع دستگاه موبایل را هسته لینوکس انجام میدهد و اندروید فقط لایه ایست که ارتباط میان کاربر وسیستم عامل را برقرار می کند.این لایه نرم افزاری به وسیله جاوا پیاده سازی شده است و به همین علت قادر به اجرای کدهای native نخواهد بود.

اندروید هماند لینوکس اوپن سورس خواهد بود و توسعه دهندگان بیشماری بر روی آن کار میکنند.

لینوکس در بین سیستم عامل های موبایل مزیت ویژه ای دارد :ارتشی از توسعه دهندگان که آماده توسعه برنامه های کاربردی برای این پلتفرم هستند.

وجود چنین جامعه بزرگی مشخص میکند که چرا فوجیستو،موتورولا ،پاناسونیک و سامسونگ به این سیستم عامل روی آورده اند. و البته مشکلی هم وجود دارد و آن ،ویرایش های مختلفی از این سیستم عامل است که توسط موتورولا و دیگرا ن ایجاد کرده اند.

برنامه هایی که روی یکی از ویرایش ها طراحی شده اند ،روی دیگر ویرایش ها کار نمی کنند.

رئیس انجمن استاندارد های تلفن های مبتنی بر لینوکس می گوید :این بزرگترین کاستی های لینوکس در مقایسه با سیمبیان و ویندوز موبایل است.

دو طرح برای استاندارد لینوکس موبایل در شرف انجام است. Access شرکت ژاپنی سازنده نرم افزارهای موبایل که Palm source سازنده سیستم عامل Palm os را تصاحب کرد در صدد معرفی پلتفرمی برای لینوکس موسوم به LINUX PLAT FORM ACCESS ، در نیمه نخست سال جاری میلادی است که استانداردهای آن توسط انجمن LISPتبیین شده است.

لینوکس سیستم عامل جدیدی است و به همان دلیل نرم افزارهای زیادی برای این سیستم عامل در بازار وجود ندارند. رواج و محبوبیت سیستم عامل ها ،فقط به توانایی و ویژگی های نرم افزاری بستگی ندارد.پشتیبانی شرکت های تولید کننده سخت افزار هم در محبوبیت ها و رواج این سیستم عامل ها هم نیز موثر لست. بر اساس آمارها نزدیک به 67 درصد از سیستم عامل های موبایل سیستم عامل سیمبین است.پس از آن ویندوز موبایل 15 درصد وپالم و لینوکس هم در مجموع 18 درصد سهام دارند.

لینوکس درصد بسیار کمی از سیستم عامل های همراه را به خود اختصاص داده است. همان گونه که در کامپیوتر شخصی.

اما رشد محسوسش نیز مانند آنچه است که بر کامپیوترهای شخصی میگذرد.جالب است بدانید از سال 2000 که اولین گوشی همراه لینوکس به بازار آمد تاکنون 33 شرکت گوشی سازی 65 مدل مختلف از گوشی های همراه لینوکس را روانه بازار کرده اند.

در میان این 33 شرکت فقط دو نام بزرگ به چشم میخورد: "موتورولا" با 17 مدل و "سامسونگ با 65 مدل.سایر نام ها ی نسبتا با سه مدل،زیمینس با یک مدل NECبزرگ در صنعت گوشی همراه لینوکس عبارتند از :فلیپس با یک مدل ،"اچ تی سی" بایک مدل ،پاناسونیک با سه مدل.این نکته حائز اهمیت است مه موتورولا و سامسونگ با وجود سیستم عامل های مختلف ،به سراغ لینوکس میروند.مسلما برتری های لینوکس بر سایر سیستم عامل های همراه بوده که موتورولا و سلمسونگ را به این سمت کشیده اند.

مزایای لینوکس همراه :

1. هزینه کمتر نسبت به سایر سیستم عامل ها
2. امنیت بسیار بالاتر بخصوص در مواجه با ویروس ها
3. به روز رسانی سریع تربه دلیل کد باز بودن
4. پایداری بیشتر

معایب لینوکس همراه

شاید بتوان تنها نقطه تاریک لینوکس همراه را در برنامه های جانبی دانست.منظور از برنامه های جانبی برنامه های جاوا نیست که اغلب روی گوشی ها قابل استفاده اند. نرم افزارهای جاوا در لینوکس به خوبی اجرا میشوند. منظوراز برنامه های جانبی نرم افزارهای مخصوص سیستم عامل است این نرم افزارها به مراتب کارائی بیشتری نسبت به نرم افزارهای جاوا دارند.به دلیل گسترش کم گوشی های لینوکس ،این برنامه ها نسبت به برنامه های سایر سیستم های عامل همراه کمترند.

# فصل دوم

# سیستم عامل اندروید

# مقدمه

اندروید را میتوان به عنوان یکی ازتاثیر گذارترین سیستم عامل های قرن حاضردانست.پا به پای ISO اندروید توانسته است راه را برای موبایل ها یی هموار کند که حرف جدیدی برای گفتن دارندو مفهومی نو از فناوری راعرضه کرده اند.در حال حاضر،اندروید گوی سبقت رااز حریفان ربوده ودرصدر پرکاربردترین سیستم عامل ها قرار دارد. این درحالی است که فعلا خبری از افول این سیستم عامل قدرتمند نیست!

در اینجا شما را بااندروید آشنا می کند وبا حقه ها وروش ها یی که در ادامه ارائه خواهند شد لذت استفاده از این اندروید رابیش از پیش برای شما آشکار می سازد.فقط اجازه دهید قبل از وارد شدن به این مباحث نگاهی به تاریخچه اندروید و همچنین تفاوت میان ورژن های مختلف آن در بازار بیاندازیم .شاید مبحث دوم به نظر خیلی مهم نرسد اما چون اندروید هر چند وقت یکبار با یک ورژن جدیدتربروز رسانی می شود آشنا شدن با پروسه ورژن ها امری حیاتی است.

# 2-1 تاریخ مختصر اندروید

کمتر از سه سال پیش زمانی که سیستم عامل اندروید برای نخستین بار توسط کنسر سیومی به رهبری گوگل معرفی شد کمترکسی پیش بینی می کرد که در این مدت کوتاه این سیستم عامل موفق به پیشی گرفتن از سیستم عامل های پر طرفداروجا افتاده تلفن همراه چون ویندوز موبایل لینوکس وپالم شد وخود را به عنوان تهدیدی جدی برای رقبایی چون سیمین RIM و آیفون نشان دهد.اندروید پارااز این هم فراتر گذاشته و علاوه برحضور در بازار تلفن های همراه هوشمند وارد عرصه های دیگری مانند تبلت ها و حتی تلوزیون نیز شده است.

به نوشته هومن کبیری رشد اعجاب آور اندروید به گونه ای بوده است که بسیاری از کارشناسان پیش بینی می کنند این سیتم عامل تاسال 2012 دومین سیستم عامل پرطرفدار تلفن های همراه جهان خواهد بود. تخمینی که نه تنها دور از دسترس نمینماید بلکه بسیار محافظه کارانه به شمار می رود. چراکه با روند رشد این سیستم عامل واقبال شرکت های مختلف به آن کسب رتبه اول به آن نیز برای اندروید چندان دور از ذهن نیست مروری خواهیم داشت بر تاریخچه و روند شکل گیری این سیستم عامل موفقیت ها و چشم انداز آتی آن.

# 2-2 معنای اندروید

پیش از ورود به اطلاعات مربوط به اندروید نخست به آن میپردازیم. بنابرترجمه دیکشنری کمبریج اندروید این گونه تعریف شده است: (( یک ربات (ماشینی که بوسیله کامپیوتر کنترل میشود) که به گونه ای ساخته شده تا شکل ظاهری شبیه به انسان داشته باشد. )) شاید بتوان نزدیک ترین معنی در زبان فارسی به اندروید را آدم آهنی یا آدم ماشینی دانست.

# 2-3 تولد یک آدم آهنی!

با اعلام زمان کنفرانس خبری شرکت گوگل در نوامبر سال 2007 دیگر تمامی رسانه ها و افکار عمومی جهان چشم انتظار مشاهده نخستین تلفن همراه ساخت گوگل بودند .ولی غافلگیری بزرگ رخ داد.هیچ خبری از ((یک)) گوشی تلفن همراه نبود بلکه خبر داغ آن روز در مورد ورود صدها تلفن همراه در سال های پیش رو بود که توسط شرکت های مختلف تولید می شد. ((اتحادیه گوشی باز)) یا Open Handset Alliance در روز 5 نوامبر 2007 اعلام موجودیت کرد. 34 شرکت فعال در زمینه تولید نرم افزار،تولید گوشی های تلفن همراه،اپراتورتلفن همراه وتولیدکننده نیمه رساناها وپردازنده های تلفن همراه اعضای مؤسس این اتحادیه بودند.در میان نام های مشهور در بین اعضای مؤسس ،شرکت ها یی چون سامسونگ ،LG،موتورولا، HTC، T-Mobile،NTT DOCOMO ،اینتل ،NVIDIA، تگزاس اینسترومنتس، کوآلکام ،برادکام،تلفونیکا،اسپرینت،EBAY و البته گوگل به چشم می خوردند .اریک اشمیت مدیر ارشد اجرایی گوگل در این مراسم گفت : ((اعلام امروز بسیار جاه طلبانه تر از معرفی تنها ((یک)) تلفن گوگلی است که در چند هفته اخیر توسط رسانه ها پیش بینی شده بود.

از دید گاه ما پلتفرمی که ما ارائه کرده ایم ،هزاران تلفن گوناگون را به بازار روانه خواهد کرد.)) نخستین گوشی مبتنی بر اندروید توسط شرکت HTC با همکاری T-MOBAIL تولید شد، این گوشی که به فاصله کمتر از یک سال از تشکیل اتحادیه OPEN HANDSET ALLIANCEیعنی در اکتبر2008 تولید شد،در بازارهای مختلف به نام های HTC DREAM،T-MOBILE ، وEra G1 به بازار عرضه گردید.

اگر عمیق تر به اندروید نگاه کنیم ،متوجه یک کرنل لینوکس می شویم .کاربرانی که گوشی هایشان راهک می کنند خوشبختا نه یا متأ سفانه باید با دستور های PROMT دست و پنجره نرم کنند اگر چه هنوز لینوکس در ژرفای آن نفس میکشد ،اما اندروید آن قدر ها هم شبیه لینوکس نیست،چون اصلا می خواهد گذشته تاریکش را فراموش کند و یک رابطکاری را ارائه کند که هر کسی از آن لذت ببرد.

در ادامه به این سؤال پاسخ می دهیم که آیا اندروید هم یکی از ویرایش های خاص لینوکس است یا خیر؟

# 2-4 آدم آهنی تقویت می شود

نهم دسامبر 2008 روز تاریخی دیگری برای اندروید بود. در این روز 14 عضو جدید از نام های معروف صنعت تلفن همراه جهان به اتحادیه open Handset Alliance پیوستند. در بین این نام ها باید به سونی اریکسون،توشیبا ،آسوس، گارمین ،هوآوی و آرم کرد. روند پیوستن شرکت های بزرگ به اتحادیه تا به امروز نیز ادامه داشته است و شرکت هایی چون ایسر ،آلکاتل ،لنوو،شارپ ،فاکسکان ، NEC، کیوسرا ،NXP، ST-Ericsson، مارول ،ZTE و دل نیز از جمله شرکت هایی بوده اند که به جمع پشتیبانی کنندگان اندروید پیوسته اند.

# 2-5 کپی رایت و حق امتیاز

حق امتیاز اندروید به صورت اپن سورس بر حق امتیاز آپاچی یا APACHE LICENS ارائه می گردد.بر این اساس شرکت های عضو اتحادیه می توانند با دسترسی به کدهای اصلی آند روید آن را مطابق دلخواه خود تغییر دهند و کد تغییر یافته را بدون عودت دادن برای خود حفظ کنند.

# 2-6 توضیح انواع مدل های اندروید

# 2-6-1 نسخه 1 و2

این نسخه ها آزمایش بوده و دارای اشکالاتی بود که میشد در نسخه های بعدی آن، این اشکالات بر طرف شود.

# 2-6-2 نسخه 1،5-CUPCAKE

نسخه 1/5 اندروید نخستین نسخه ای بود که به طور رسمی منتشر شد.این نسخه اندروید مبتنی بر کرنل لینوکس 27و6و2 بود. ازجمله قابلیت هایی که در این ویرایش گنجانده شده بود ،باید به موارد زیر اشاره کرد:

1. امکان ضبط فیلم از طریق دوربین فیلم برداری آن
2. فرستادن فیلم به سایت YOUTUBE وعکس به سایت PECASAبه صورت مستقیم ازروی گوشی .
3. صفحه کلید مجازی با قابایت پیش بینی کلمات وارد شده.
4. پشتیبانی از پخش استریوی موسیقی از طریق بلوتوث (A2DP ) وکنترل پخش موسیقی یا ویدیواز طریق بلوتوث ( . (AVRCPRقابلیت اتصال اتوماتیک به دستگاه های بلوتوث.
5. امکان شخصی سازی صفحه اصلی با استفاده از ویجت ها ویا پرونده های شخصی.
6. جابه جایی انیمیشنی تصاویر به هنگام عوض شدن صفحات.

# 2-6-3 نسخه 6و1 –DONUT

در 15 سپتامبر2009 اندروید نسخه 1/6 یا دونات منتشر شد.این نسخه اندروید مبتنی بر کرنل لینوکس نسخه 29و6و2 بود و قابلیت های زیر را به اندروید افزود:

1. بهبود در سرویس اندروید مارکت
2. رابط کاربری یکپارچه برای دوربین عکسبرداری ،دوربین فیلمبرداری و گالری تصاویر
3. امکان انتخاب چند عکس برای پاک کردنددر منوی گالری
4. به روز رسانی ویژگی جست وجوی صوتی
5. به روز رسانی ویژگی جست جو با قابلیت جستجو در موارد نشانه گذاری شده (BOKMARKS )، تاریخچه((HISTORY، اسامی (CONTACTS ) و وب از صفحه اصلی(SCREEN HOME)
6. پشتیبانی از تکنولوژی های به روز شده CDMA/EVDO ،1، 802،VPN وموتور TEXT TO SPEECH
7. پشتیبانی از تکنولوژی WVGA برای صفحه نمایش
8. افزوده شدن قابلیت های حرکتی در سیستم عامل و ابزار برنامه نویسی برای برنامه نویسان

# 2-6-4 نسخه 2 و 1،2

هر دو نسخه 2و2/1 اندروید مانند نسخه 1/6 مبتنی بر کرنل لینوکس 2،6،29 طراحی شده اند. اندروید ویرایش 2 در 26 اکتبر 2009 معرفی شد.در سوم دسامبر2009SDK نسخه 1،0،2 معرفی شد و SDK ویرایش 2/1 در 12 ژانویه 2010 منتشر گردید.

اهم امکانات اضافه شده به شرح زیر هستند:

* سرعت سخت افزاری بهبود یافته
* ویژگی چند لمسی MULTI TOUCH
* پشتیبانی از رزولوشن های بیشتر برای صفحه نمایشس
* رابط کاربری به روز رسانی شده
* مرور گر اینترنتی با قابلیت پشتیبانی ازHTML 5
* دفترچه تلفن بروز رسانی شده
* گوگل مپ نسخه 3،1،2
* پشتیبانی از MICROSOFT EXCHANGE
* افزوده شدن امکان فلاش داخلی برای دوربین
* به روز رسانی صفحه کلید مجازی
* پشتیبانی از بلوتوث نسخه 2/1
* اضافه شدن قابلیت کاغذ دیواری های متحرک
* اضافه شدن امکان ارسال فایل با استفاده از بلوتوث

# FROYO 2-6-5 نسخه 2،2

اندروید نسخه 2،2 در 20 مه 2010 معرفی شد.این ویرایش اندروید مبتنی بر کرنل لینوکس نسخه 32،6،2 است و قابلیت های زیر به آن اضافه شده است :

* افزایش سرعت سیستم عامل ،حافظه و عملکرد سیستم بین 2 تا 5 برابر نسخه 2
* افزایش سرعت اجرای برنامه های کاربردی با استفاده از تکنیک های JIT
* اضافه شدن موتور جاوا اسکریپ V 8 کروم به مرورگر اینترنتی
* افزایش پشتیبانی از MICROSOFT EXCHANGE با قابلیت هایی چون سیاست حریم شخصی به روز شده ،همسان سازی تقویم و ...)
* اندروید مارکت به روز شده با قابلیت به روز رسانی خودکار برنامه های کاربردی
* شماره گیری صوتی و انتقال دفترچه تلفن از طریق بلوتوث
* امکان نصب برنامه های کاربردی بر روی حافظه های جانبی
* پشتیبانی از فلش نسخه 10/1 بهبود عملکرد دوربین در حالت های عکس وفیلمبرداری

# GINGERBREAD 2-6-6 نسخه 2،3

نسخه 2،3 در روز دسامبر سال 2010 میلادی معرفی شد . بر جسته ترین ویژگی معرفی شده در این نسخه جدید، پشتیبانی از تراشه های NFC (NEAR –FIELD-COMMUNICATION) است. اولین گوشی موبایل که به همراه این نسخه از سیستم عامل عرضه شد یعنی NEXUS S شرکت سامسونگ ،به این تراشه نامریی NFC مجهز بود .تراشه های NFC اساسا می توانند تلفن شما را به نوعی کارت اعتباری تبدیل کنند. در شرایط ایده آل ،وقتی شما تلفن خود را مقابل سنسور ویژه یک فروشگاه حرکت می دهید ،مبلغ خریدتان بلافاصله پرداخت خواهد شد. البته هنوز هیچ راهی برای آزمایش ویژگی مذکور در دنیای واقعی وجودندارد، زیرا هیچ برنامه ای از پرداخت های موبایل پشتیبانی نمی کند.کاربران زیاذی با صفحه کلید استاندارد اندروید گوگل مشکل دارشته اند .در واقع کلید های تعبیه شده روی صفحه کلید استاندارد برای بسیاری از ما آ ن قدر کوچک و فشرده هستند که به راحتی امکان تایپ یک متن طولانی را فراهم نمیکنند.

اندروید 2،3 شکل کلید های صفحه کلید را تغییر داده تا به جای مربع بیشتر به مستطیل شباهت داشته باشند. از سوی دیگر ،حالا فاصله بیشتری در بین کلیدها وجود دارد .شما بلافاصله متوجه خواهید شد که استفاده از طراحی جدید کلیدها بسیار راحت تر است.یکی از نکات جالب توجه در صفحه کلید نسخه جدید اندروید این است که شما می توانید به طور همزمان کلیدSHEFT و هرکلید حرفی را فشار دهید تا یک سمبل یا عدد را به دست آورید ودیگر نیازی ندارید که بین حالت های مختلف سوئیچ کنید.

ویژگی جذاب نسخه جدید این است که شما می توانید از صدای خود در هنگام تایپ برای تصحیح عبارات استفاده کنید . کافی است انگشت خود را روی عبارت گذاشته و نگهدارید،حالا کلید اختصاصی کنترل صوتی ( که به یک میکروفون شباهت دارد )را روی صفحه کلید خود انتخاب کنید. اکنون می توانید عبارت صحیح را انتخاب کرده و امیدوار باشید که اندرویدآن را می فهمد.این ویژگی در آزمای ش های انجام شده به خوبی کار می کرد،اما بعید به نظر می رسد که تعداد زیادی از کاربران از آن استفاده کنند. برنامه کنترل دوربین نیز در نسخه جدید تغییر کرده و می توان گفت که استفاده از آن ساده تر و کارآمد تر شده است. این برنامه به شما امکان می دهد که به آسانی هر دو دوربین پشتی و جلویی گوشی خود را کنترل کنید.اندروید 2،2 به طور محسوسی سریع تر از نسخه 2،1 این سیستم عامل بود،اما برتری مذکور به بهای کاهش عمر باتری ابزار به دست می آمد. گوگل با برطرف کردن این مشکل ،نسخه 2،3 اندروید را طوری بهینه سازی کرده که بازدهی مصرف برق بهتری داشته باشد.نرم افزار در عین حال یک منوی آراسته باتری را در اختیار شما می گذارد که نشان می دهد چقدر از توان باتری خود استفاده می کنید وابزار شما پیش از نیاز به شارژ احتمال برای چه مدتی به کار خود ادامه خواهد داد.در مجموع می توان گفت که گوگل تلاش می کند تا عملکرد زیر بنایی سیستم عامل خود را بهبود بخشد. با توجه به رقابت شدیدی که در حوزه سیستم های عامل جریان دارد وسود سر شاری که در این بازار توسعه دهندگان می شود،گوگل به هیچ وجه حاضر نیست جایگاه خود را به خاطر یک اشتباه کوچک از دست بدهد.

# Honeycomb2-6-7 نسخه 3 و3،1 و3،2

HONEY COMB یا کندوی عسلی ،که این نسخه تغییرات زیادی را نسبت به ورژن های گذشته در خود نداشت و به نوعی یکی از نسخه های بی سروصدای اندروید نام گرفت و بیشتر درتبلت ها به کار گرفته شد.

# Ice Cream Sandwich 2-6-8 نسخه 4

نسخه جدید اندروید با نام Ice Cream Sandwich یا بستنی حصیری در اکتبر 2011 بر روی نکسوس جدید Galaxy Nexus معرفی و روانه بازار گشت.این نسخه تغییرات بسیار زیادی را خصوصا از نظر ظاهری و رابط کاربری نسبت به دیگر نسخه های دیگر در خود گنجانده است،این تغییر را بیشتر کسانی متوجه می شوند که تلفن خود را از ورژن قبل به این نسخه بروز رسانی کرده باشند.

گوگل در کنفرانس I/O 2012 سانفرانسیسکو آخرین سری از نسخه اندروید را معرفی و پرده برداری کرد.گوگل این نسخه را Jelly bran یا همان لوبیای (آب نبات )ژله ای نام گذاری کرد .این نسخه ویژگی و قابلیت های فراوانی دارد که تا به حال این سیستم عامل در تبلت گوگل و ایسوس با نام

ASUS GOOGLE NEXUS 7 وگلکسی نوت 2 استفاده شده است.

* مرکز اطلاعات و هشدارهای بهبود یافته
* ویجت های جدید
* بهبود عملکرد صفحه کلید(حدس کلمات)
* تشخیص صدا و تایپ آفلاین
* جستجوی صوتی گوگل با امکانات بیشتر نسبت به ورژن های قبل
* به روز شدن رابط کاربری GOOGLE SEARCH
* اضافه شدن فید های اطلاعاتی به دستگاه شما از قبیل ترافیک،آب وهوا،ورزش و...
* پشتیبانی از زبان های بیشتر
* ساپورت از خروجی صدااز طریق USB و HDMI
* قابلیت رمز گذاری و بروز رسانی هوشمند نرم افزارها

توجه کنید که دستگا ه ها به طور اتوماتیک توسط گوگل آپدیت نمی شوند و به سازنده دستگاه بستگی دارد. چطور می توانید بفهمید ورژن حال حاضر گوشی شما کدام است؟ بسیار ساده است ! از صفحه خانگی ،دکمه منو را فشار داده وسپس به قسمت تنظیمات بروید.از آنجا به قسمت درباره گوشی بروید و اطلاعات نرم افزاری را انتخاب کنید. در ابتدای این اطلاعات ورژن اندروید شما مشخص شده است.

# 2-7 میزان محبوبیت نسخه های مختلف اندروید

در ابتدا باید بگوییم که نسخه بستنی حصیری توانسته در آمار وارقام جدید بیشترین رشد را داشته باشد. در ماه ژوئن فقط7،1 درصد از گوشی های اندرویدی مبتنی بر بستنی حصیری بوده اند که این رقم برای ژوئیه به 15،9 درصد رسیده است. با این حال باز هم نسخه های 2،3 و2،3،7 بیشترین عدد را به خود اختصاص داده اند وبا60،6 درصد در صدر جدول قرار دارند والبته نسخه 2،2 اندروید یعنی با FROYO با 15.5درصد در پشت سر بستنی حصیری قرار گرفته است.در حال حاضر95 درصد از کاربران اندروید از نسخه های 2و2 به بالا بهره می گیرند.در ماه های آینده نیز به علت عرضه گوشی های هوشمند بیشتری با نسخه 4,0 اندروید باید منتظر رشد بیشتری بستنی حصیری باشیم ودر پایین ترین سطح آمار نسخه JELLY BEANS فقط 0,8 درصد از این بازار را در اختیا ر دارد،نسخه ای که بی تردید با افزایش روز افزونی مواجه خواهد شد.

# 2-8 سرعت انتشار ویرایش های اندروید فرصت ها وتهدید ها

اندروید با سرعت اعجاب آوری در حال پیشرفت است. این امر باعث شده تا تنها برخی از شرکت ها که به طور متمرکز و با تمام توان بر روی این سیستم عامل کار می کنند،مانند موتورولا و HTC،بتوانند همگام با ارائه ویرایش های جدید اندروید گوشی های خود رابه روز کنند ولی سایر شرکت ها رفته رفته در حال عقب افتادن از این قافله هستند.به عنوان مثال باید به شرکت سونی اریکسون اشاره کرد.

این شرکت نخستین گوشی اندرویدی خود را با نام XPERIA X10 که مبتنی براندروید نسخه 1/6 است،به بازار معرفی کرد.سونی اریکسون رابط کاربری ویژه خود و امکانات ابتکاری فراوانی به X10 افزوده است. اوایل بهار سال جاری سونی اریکسون با خوشحالی اعلام کرد که قصد داردتا پایان سال جاری میلادی گوشی های X10 خود را بانسخه 2/1 اندروید به روزرسانی کند.کمتر از دو هفته بعد ز نسخه 2/2 اندروید منتشر شد وشرکت های موتورولا و گوگل در همان زمان اعلام کردند که گوشی های اندروید و نگزوس وان خود را تا یک ماه بعد به اندروید 2/2 مجهز خواهند ساخت.

اتفاقی که شاید 6 ماه بعد برای X10 سونی اریکسون بیفتد ! چنین وضعیتی برای شرکت های بزرگی چون سامسونگ و ال جی نیز وجود دارد.ای شرکت ها هم هنوز نتوانسته سرعت واکنش خودرا با سرعت سرسام آورپیشرفت اندروید هماهنگ سازند.درصورتی که این شرکت ها نتوانند به چنین هماهنگی دست یابند،شکاف بین تولید کنندگان پیشروی اندروید یعنی موتورولا و HTC با بقیه بسیار بیشتر خواهد شد.

در هر حال به نظر می رسد گوگل باید فکری به حال فاصله ایجاد شده بین رقبا بکند وگرنه بروز این ناهماهنگی بازار را نیز دچار آ شفتگی خواهد کرد. همان گونه که در سطور پیشین نیز ذکر شد در حالی که گوگل خود را برای ارائه نان زنجفیلی یعنی نسخه بعد از 2/2 اندروید آماده می کرد ،هنوز نیمی از دستگاه های اندروید فعال ،از نسخه پایین تر از 2/1 استفاده می کردند واین بدان معنااست که گوگل بسیار سریع تر از یارانش دراتحادیه OPEN HANDSET ALLIANCE حرکت کرده است وآنها نتوانسته اند خود را با آن همراه سازند.

# 2-9 سهم بازار اندروید

سهم بازار اندروید در مقایسه با سایر سیستم های عامل تلفن های هوشمند ،رشد اعجاب آور اندروید را نشان می دهد.اندروید برای نخستین بار در سه ماهه اول سال 2010 توانست گوشی های بیشتری از مهم ترین رقیب خود یعنی اپل به فروش برساند. برخی کار شناسان بر این باور هستند که اگر گوگل موفق شود اپل را از پیش روی خود بردارد RTM سیمبین را نیز پشت سر خواهد گذاشت. گروهی از کارشناسان ،استراتزی اندروید درمقا بله با اپل را با استراتژی مایکروسافت در اوایل دهه 1970 مقایسه می کنند.

جایی که مایکروسافت توانست با فروش حق امتیاز استفاده از سیستم عامل خود به سایر شرکت ها به سلطه مکینتاش خاتمه دهد وحالا گوگل به همین استراتژی و به کمک بزرگترین تولید کنندگان تلفن همراه مانند سامسونگ ،ال جی ،سونی اریکسون، موتورولا و اچ تی سی،قصد دارد روند رشد آیفون اپل را متوقف سازد و به نظر می رسد تا حد زیادی هم موفق بوده است.براساس آمار ارائه شده توسط شرکت ADMOB در آوریل 2010 تعداد گوشی های آیفون موجود در بازار ایالات متحده آمریکا 10/7 میلیون دستگاه بوده است. این در حالی است که تعداد گوشی های مبتنی بر اندروید 8/7 میلیون دستگاه بوده است .ذکر این نکته ضروری است که نخستین گوشی آیفون در 29 ژوئن 2007 به بازار عرضه شد در حالی که نخستین گوشی مبتنی بر اندروید بیش از یک سال بعد ودر اکتبر 2008 روانه بازار شد. اما به غیر از اپل بقیه رقبا نیز از دست اندروید جان به در نبرده اند.

اندروید در سه ماه نخست سال 2010 توانست سهم بازار خود را از 1/6 درصد در مدت زمان مشابه در سال گذشته به 9/6 درصد برساند وبا پشت سر گذاشتن ویندوز موبایل و لینوکس در رده چهارم پر طرفدار ترین سیستم عامل تلفن های همراه هوشمند قرار گیرد.

با اقبال بیشتر سایر تولید کنند گان به گوشی های اندروید به نظر می رسد روند رشد این سیستم عامل نه تنها کند نگردد بلکه شتاب بیشتری نیز پیدا کند .تا کنون بالغ بر 61مدل دستگاه مبتنی براندروید با 21 برند مختلف تولید شده است. بنابر آخرین گذارش ها در حال حاضر هر روز یکصد هزار گوشی مبتنی بر اندروید به فروش می رساند .با نرخ کنونی گوگل 36 میلیون گوشی در سال به فروش خواهد رساند.این رقم زمانی معنا پیدا می کند که بدانیم شرکت اچ تی سی، چهارمین تولیید کننده تلفن های همراه هوشمند در جهان سالانه 17 میلیون گوشی تلفن همراه به فروش می رساند. اچ تی سی پیش از این 70 درصد گوشی های مبتنی بر اندروید را تولید می کرد.

رقمی که اکنون به زحمت به 50 درصد می رساند.با نرخ کنونی ودرصورت ثابت ماندن نرخ فروش آیفون ، اندروید خواهد توانست اپل را نیز پشت سر گذاشته و خود را به عنوان تهدیدی جدی برای RIM مطرح کند .شرکت های بزرگ تولید تلفن همراه اعلام کرده اند قصد دارند تولید گوشی های مبتنی بر اندروید را شتاب بخشند. فعال ترین گوشی های مبتنی بر اندروید یعنی موتورولا اعلام کرده اند تا پایان سال جاری میلادی 20 مدل گوشی مبتنی بر اندرویدبه بازار عرضه خواهد نماید. سامسونگ دومین تولید کننده تلفن های همراه در جهان هم اعلام کرد نیمی از گوشی های تلفن همراه هوشمند این شرکت در سال 2010 مبتنی بر اندروید خواهد بود. بقیه تولید کنندگان هم هر روز علاقه بیشتری به تولید گوشی های تلفن همراه مبتنی بر اندروید از خود نشان می دهند .با این اوصاف انتظار می رود اندروید بتواند جهشی شگرف در سهم بازار را رقم زند.

# 2-10 دستگاه های شاخص مبتنی بر اندروید

در بین شرکت های تولید کننده تلفن های همراه هوشمند مبتنی بر اندروید دو شرکت موتورولا و HTC تحرک بسیار گسترده تری نسبت به سایر رقبا دارند. موتورولا که زمانی دومین تولید کننده تلفن همراه جهان بود،پس از زیان دهی در دوره های مالی متوالی و کاهش چشم گیر سهم بازار در موقعیتی بهرانی قرار گرفته بود ،با تغییر ناگهانی استراتژی خود و کنار نهادن سایر سیستم های عامل تلفن همراه از قبیل ویندوز موبایل ،سیمبین و لینوکس موبایل ،تمامی تلاش خود را بر طراحی گوشی های مبتنی بر اندروید معطوف ساخت .

این شرکت توانست با استراتژی جدید خود چندین مدل گوشی هوشمند مبتنی بر اندروید به فروش برساند و با این کار پس از مدت ها سود آوری را تجربه کند .موتورولا رابط کاربری ویژه اندروید مختص به خود را با نام MOTOBLUR طراحی کرده وبر روی گوشی های خود قرار داده است .به نظر می رسد با توجه به توانمندی های این شرکت که خالق تلفن همراه به شمار می رود ،بتوان از هم اکنون موتورولا را طلایه دار اندروید دانست. به خصوص HTC هم باید گفت هر چند این شرکت به موازات تولید گوشی های مبتنی بر اندروید به تولید گوشی های با سیستم عامل ویندوز موبایل هم میپردازد ولی رفته رفته ،توان خود را بیشتر بر تولید گوشی های مبتنی بر اندروید هدایت می کند .

HTC علاوه بر تولید گوشی با برند خود به تولید گوشی های با برند سایر شرکت ها هم میپردازند و گوشی نگزوس وان شرکت گوگل یکی از همین نمونه ها است .گوگل تولید نخستین گوشی با نام تجاری خود را پس از اینکه شرکت سونی اریکسون از تولید آن با برند گوگل سرباز زد به HTC سپرد.بنابر آخرین آمار ارائه شده ازسویADMOB بر اساس اطلاعات ترافیک دیتای ماه مارس 2010 ،چیزی در حدود یک سوم تلفن های همراه فعال مبتنی بر اندروید ،مدل دروید شرکت موتورولا هستند.پس از دروید گوشی های مدل HERO با 19 درصد ،DREAM یا همان T-MOBILE با 11 درصد و MAGIC هم با 11 در صد در رده های بعدی قرار دارند.

# 2-11 اندروید مارکت

اندروید مارکت سرویس فروش نرم افزار های کاربردی برای گوشی های اندروید است.یک برنامه کاربردی ویژه اندروید مارکت به صورت از پیش بار گذاری شده بر روی گوشی های اندروید نصب گردیده و به کا ربران امکان می دهد نرم افزارهای مورد نیاز خود را خریداری ودانلود کنند. البته تمامی نرم افزار های موجود در اندروید مارکت فروشی نیستند بلکه بیش از نیمی از نرم افزارهای موجود در اندروید مارکت به صورت رایگان عرضه می شوند واز این نظر اندروید بیشترین درصد نرم افزار های رایگان را در بین تمامی سیستم عامل تلفن های همراه هوشمند در اختیار کار بران قرار می دهد.

هر برنامه نویس با ثبت نام ،امکان فروش برنامه های خود در اندروید مارکت را دارد.70درصد از مبلغ فروش برنامه های کا ربردی به برنامه نویس تعلق می گیرد و 30 درصد مابقی بین اپراتورها توزیع می شود. براساس سیاست های گوگل در حال حاضر تمامی برنامه نویسان عضو پروژه اندروید از سراسر جهان می توانند برنامه های کاربردی رایگان خود را از طریق اندروید مارکت در 46 کشور عرضه کنند. برای اینکار کافی است برنامه نویسان فرمی مختصر را تکمیل کرده و البته 25 دلار حق عضویت هم به گوگل بپردازند.

ولی تنها برنامه نویسان ساکن در نه کشور اتریش،فرانسه،آلمان ،ایتالیا،ژاپن، هلند،اسپانیا،انگلستان وایالت متحده آمریکا می توانند برنامه های خود را برای فروش در 13 کشور اسنرالیا، اتریش، کانادا، فرانسه، آلمان، ایتالیا، ژاپن، هلند،نیوزلند،اسپانیا،سوییس،انگلستان و ایالات متحده آمریکا در معرض بازدید خریداران قرار دهند وسایر کشورها امکان مشاهده و خرید برنامه های غیر رایگان را ندارند.

نکته جالب توجه در این زمینه عدم حضور حتی یک کشور از منطقه خاور میانه و شمال آفریقا (به غیراز اسرائیل )در لیست چهل و شش کشوری است که امکان دسترسی به اندروید مارکت را دارند! این در حالی است که گوشی های مجهز به اندروید از سوی اغلب شرکت های بزرگ از جمله موتورولا ،HTC ، سونی اریکسون ،و ال جی در این منطقه مدت ها است که به بازار عرضه شده اند.تعداد برنامه های کاربردی موجود در اندروید مارکت تا کنون نزدیک به 50000 بوده است این در حالی است که برنامه های کاربردی موجود در ITUNE برای گوشی آیفون 175000 برنامه بالغ می شود و از این منظر به نظر می رسد که اندروید راهی دراز برای سبقت گرفتن از آیفون در پیش دارد. ولی در هر حال باید این نکته را هم در نظر داشت که هر چند تعداد برنامه های کاربردی نشانگر اقبال برنامه نویسان به پلت،فرم مورد نظر است،ولی تعداد بسیار زیاد برنامه ها برای کاربران همیشه هم خوب نیست.چرا که آنان را مجبور می سازد تا جستجویی سخت و طاقت فرسا را برای دستیابی به برنامه مورد علاقه خود تجربه کنند . گوگل کوشیده است دسترسی به برنامه های کاربردی اندروید را به شدت محدود ساخته و تمامی دسترسی کاربران را از طریق نرم افزاراندروید مارکت نصب شده بر روی گوشی کاربران کانالیزه نماید. گوگل تا بدانجا پیش رفته است که حتی دسترسی به اطلاعات و امکان جستجوی برنامه های کاربردی اندروید از وب سایت رسمی اندروید مارکت از طریق کامپیوترهای شخصی، امکانپذیر نیست.

از طرف دیگر عدم امکان نصب نرم افزارهای دانلود شده بر روی کارت حافظه محدودیت دیگری است که کاربران برای دانلود برنامه ها از هر جای دیگری به غیر از اندروید مارکت با آن مواجه هستند.اما هنوز هم راه هایی برای دور زدن گوگل برای دستیابی به برنامه های کاربردی وجود دارد .بسیاری از برنامه نویسان از جمله شرکت های تولید برنامه های کاربردی نسخه قابل نصب برنامه های خودرا علاوه بر اندروید مارکت از طریق وب سلیت های خود نیز دراختیار کاربران قرار می دهند.علاوه بر این برخی وب سایت ها اقدام به جمع آوری و در اختیار قرار دادن برنامه های کاربردی پرطرف دار اندروید نموده اند. نمونه ای از این سایت ها ANDROIDZOOM وANDROLIB هستند.همچنین با نصب یک نرم افزار بر روی گوشی خود امکان خواهید یافت برنامه های دانلود شده بر روی کارت حافظه خود را بر روی گوشی نصب نمایید.اگر چه با استفاده از راه هایی که گفته شد امکان نصب برخی نرم افزار ها بر روی گوشی خود را خواهید داشت ، ولی باید اذعان کرد که اغلب برنامه های اندروید به ویژه برنامه های اصلی آن که توسط خود گوگل طراحی شده اند، مانند نقشه های گوگل یا برنامه گا گلز ) (GOGGLE تنها از طریق اندروید مارکت قابل دسترسی هستند .پس اگر می خواهید به برنامه های کاربردی اصلی اندروید دسترسی داشته باشید ،باید از اندروید مارکت نصب شده بر روی گوشی خود استفاده کنید.

# 2-12 تم انحصاری سازندگان

گوگل به سازندگان این شانس را داده است تا آن ها بتوانند هر قسمتی ازاین سیستم عامل را تغییر بدهندوهمین طور رابط کاربری و یا پوسته ای ارائه می دهند که در وهله اول منحصر به فرد ودر وهله دوم متفاوت از سایر رقبا باشد. برای مثال اخیرا سامسونگ به خاطر رابط کاربی اش ،TOUCHWIZ در آستانه اتهام بزرگی قرار گرفت چون اپل فکر کرد سامسونگ از IOS تقلید کرده است . خوشبختانه هیچ سازنده دیگری از طرق اپل مورد اتهام قرار نگرفت چون رابط کاربری آن ها کاملا متفاوت بود.

درموردهمین رابط کاربری ،باید بگویم که هیچ منوی خاصی در اندروید تعبیه نشده است تا به شما ورژن رابط کاربری را اعلام کند.در عوض ،می توانید با تکیه بر سازنده گوشی،آن اطلاعات را به دست بیاورید.رابط کاربری HTC به نام SENSE است واین در حالی است که رابط کاربری MOTORPLA اخیرا با نام MOTOBLUR منتشر شده است که بعد به NINJA BLUR تغییر نام دادو حالا هم هیچ نام رسمی ای ندارد!بهترین مکان برای دریافت اطلاعات تغییرات رابط های کاربری سازندگان ،وب سایت آنهاست و این در حالی است که بیشتر خصوصی سازی ها در زیر پوست اندروید سازندگان پنهان است.این خصوصی سازی ها هیچ تأثیری بر اجرای نرم افزارها نداردو فقط ظاهر را تغییر می دهد که در بخش دوم به آن پرداخته خواهدشد.

# 2-13 رابط کاربری صفحات خانگی

همه گوشی های اندروید از یک صفحه خانگی پایه استفاده می کنند . این صفحه خانگی را می توان به طور جذاب تری،" دسکتاپ اندروید " ،نام گذاری کرد.این دسکتاپ مکانی است که آیکون های شما آن جا زندگی می کنند وهمین طور مکانی است برای دسترسی به مهم ترین قسمت های گوشی است. این شامل APPS DAWER و تنظیمات گوشی هم می شود.

صفحه خانگی در حالی یکی از قسمت های رابط کاربری به شمار می رود که آیکون های اختصاصی اندروید رادر خودجای داده است.با نام HOME KEY ،معمولا با یک آیکون کوچک و جذاب از یک خانه به نمایش در می آید.

# 2-14 آیکن ها

به طور پیش فرض ،وسایل اندرویدی از یک شبکه از پیش تعیین شده برای جا دادن آیکون ها (برای گوشی های 304 اینچی این اندازه 4 در 4 است ) بر خوردارند. آن چنان انعطا ف پذیر است این اندروید که می توانید با لمس کردن و تکان دادن آیکون ها مکان آن ها را تعیر دهید. در این شرایط ، شبکه آیکون ها در برابر تنظیمات از اولویت بیشتری بر خوردار است ،چون صرف نظر از تنظیمات ،آیکون ها در چار چوب شبکه محدود خواهند بود. وقتی آیکونی را رها می کنید ،به طور اتوماتیک مکان مناسب خودش را پیدا خواهد کرد و خودش را جا خواهد داد!

با باز کردن APP DRAWER می توان آیکون های جدیدی را اضافه نمود به این صورت که آیکون جدید توسط کار بر لمس خواهد شد و بعد از ناپدید شدن برنامه، صفحه خانگی به نما یش در خواهد آمد . همچنین ،بردن آیکون ها به لبه صفحه این امکان را به شما می دهد تا آیکون ها را صفحات خانگی بعدی منتقل کنید.

# 2-15 پوشه ها

اندروید از ورژن 5.1 تا حالا از پوشه ها استفاده می کند. با یک لمس طولانی در یک قسمت خا لی از صفحه خانگی ، متویی ظاهر خواهد شد که تنظیمات پوشه ها در آن قرار دارد. انتخابFOLDER New یک پوشه جدید را ایجاد خواهد کرد که میتوانید بعد آن را به هر جایی که خواستید منتقل کنید .حتی میتوان نرم افزارها را به داخل پوشه ها منتقل کرد. در این صورت باز کردن پوشه ،نرم افزار انتقالی ظاهر خواهد شد.در صورت نا رضایتی ( ! )، میتوان آن ها را به جای قبلی باز گرداند و مشکلی از این بابت نیست.قراردادن فایل ها دریک پوشه سخت تر از این حرف هاست .پوشه ها می توانند میزان خوبی برای فایل ها باشند،اما مشکل اینجاست که هیچ برنامه مدیریت فایل از پیش نصب شده ای بر روی پیشتر گوشی های اندرویدی وجود ندارد.با وجود این ،شما نیز به دانلود یک برنامه مدیریت فایل خواهید داشت،مثل ASTRO FILE MANAGER .بعد می توانید با استفاده از برنامه ،فایل ها را به عنوان SHORTCUT به صفحه خانگی اضافه نمایید که آن SHRTCUT میتواند داخل یک پوشه قرار بگیرد.

# 2-16 ویجتها

اگر قابلیت وجود داشته باشد که تجارت کاربران اندروید را درخشان سازد،آن ویجت ها هستند.یک ویجت ،یک عنصر واسط کاربری است که اساسا در صفحه خانگی گوشی قرار داردو امکاناتی را بدون نیاز به داشتن پروسه فعال دراختیار کاربر قرار می دهد این ویجت ها قادرند تا امکاناتی از قبیل اطلاعات آب و هوا ،آپدیت های دوستان در فیسبوک و یا نمایش تقویم را در اختیار شما بگذارند.اگر چه ،عملکرد همه این ویجت ها در یک چارچوب خاص قرار دارد،از لحاظ تعداد،ویجت ها آنقدر زیاد هستند که حتی توضیحات آنها در یک کتاب 100 هزار صفحه ای جا نمی شود،چون هر سازنده ای ویجت های خاص خودش را تولید می کند و همینطور اندروید مارکت هم تعداد زیادی از ویجت ها را در خود جا داده است.آن ها ،فضایی را در شبکه صفحه خانگی اندروید اشغال می کنند و می توانند منتقل و یا حذف شوند.

وجت ها هم چنین با یک روش اضافه می شوند . برای اضافه کردن یک ویجت ،در یک فضای خالی از صفحه خانگی ، انشگتتان را فشار دهید وهنگامی که منویADD TO HOME SCREEN ظاهرشد،منوی WIDGETS را باز کنید تا با لیستی از ویجت های قابل نصب مواجه شوید.بیشتر گوشی های اندروید ،اجازه تغیر ساز ویجت ها را نمی دهند وهمین ،باعث شده است تا ویجت ها با سایز های مختلفی ارائه شوند. اگر چه،اجرا کننده های اختصاصی ،این امکان را فراهم کرده اند.

# 2-17 فواید اجرا کننده های اختصاصی

در نگاه اول ،گوشی های هوشمند اندروید ،با فراهم کردن امکانات یک کامپیوتر بر روی یک فضای نه چندان بزرگ ،حیرت فناوری به نظر می آیند.خیلی ها،مدت زیادی این باور را با خود به همراه دارند،اما بسیاری از خوره های فناوری از معایب نه چندان جالب،مثل اندازه شبکه محدود برای آیکون ها و پوشه ها رنج می برند!

در این شرایط است است که یک اجرا کننده اختصاصی به کار می آید.از نامش برمی آیدکه فقط به درد اجراکردن برنامه ها بخورد،امااین اجرا کننده اختصاصی به کار می آید. از نامش بر می آید که فقط به درد اجرا کردن برنامه ها بخورد،امااین اجرا کننده ها به شما این امکان را می دهند تا صفحه خانگی اندروید خود را طبق میل خود آرایش کنید.امکاناتی از قبیل :تغییر سایز آیکون های شبکه،ویرایش تعداد صفحات خانگی و...

این اجرا کننده ها هر کدام قابلیت های متفاوتی را ارائه می دهند،اما به هر حال با استفاده ازآن ها می توانید اندروید شخصی خودتان را داشته باشید! بعضی از این اجرا کننده ها عبارتنداز: LAUNCHERPRO، ADW LAUNCHER و REGINA 3D LAUNCHER استفاده از این برنامه ها ،اولین قدم برای اختصاصی سازی اندروید است.

# 2-18 لذت چند رسانه ای و مدیریت

نرم افزار های مدیریت رسانه تقریبا هر کسی می داندکه گوشی های هوشمند لمسی،با پخش کننده های قدرتمند،تجربه ای لذت بخش رابرای کاربران فراهم می آورند.وقتی که شما یک گوشی هوشمند داشته باشید،دیگر یکMP4 یا MP3 عتیقه به حساب می آیند! وبرای این که بتوانید تمام وکمال از این امکانات لذت ببرید،باید در وهله اول یک برنامه مدیریت پخش توپ داشته باشید ،اگر چه بیشتر گوشی های اندرویدی از نداشتن این گونه برنامه ها رنج می برند!

گزینه صحیح ،کامل ترین گزینه است .من شخصا ازWINAMP خوشم می آید. شاید انتخابم از روی تعصب باشد چون برای سال ها از این برنامه بر روی کامپیوترم هم استفاده کرده ام و یا رویاور من در پخش بوده است .این برنامه ،یکی از معدود برنامه های اندروید است که هم از ویدئو پشتیبانی می کند و هم موزیک.جالب تر این که این برنامه رایگان است! بااین وجود ،ظاهرا به این برنامه ظلم شده است!برنامه ای مثل MIXZING تقریبا همه فایل های صوتی را پخش می کند واز قابلیت نمایش نوت موزیک هم برخوردارد است.همچنین یک ویجت برای قفل کردن صفحه نمایش هم در این برنامه به چشم می خورد که به شما امکان کنترل پخش کننده را بدون نیازبه باز کردن گوشی می دهد .اگر چه این نرم افزار تنها $ 4.99 قیمت دارد،اما به نظر می رسد کسانی که از گوشی خود به عنوان یک MP3 PLAYER استفاده می کنند،به راحتی بتوانند این هزینه را پرداخت کنند.

برنامه دیگری که می توانیم از آن نام ببریم ،برنامه PODCAST MANAGER است. پادکست ها به راحتی بر روی گوشی ها دانلود می شوند،اما مدیریت آن ها کمی دشوار است. نرم افزارهای مدیای معمولی در سازمان دهی آن ها با مشکل مواجه هستند.به همین منظور ،برنامه های مدیریت پادکست به کاربران اجازه ی پیش نمایش ،دانلود، سازمان دهی و گوش کردن به پادکست ها را می دهند.من شخصا از BEYONDPAD استفاده می کنم.انتخاب دیگر می تواند MYPOD PODCAST MANAGER باشدکه اجازه سازمان دهی بیش از 10 پادکست رادر یک زمان می دهد.امااین ها تنها گزینه های شما نخواهند بود. در مقاله بهترین نرم افزارهای اندروید نرم افزارهای متعددی در موضوعات مختلفی از جمله پخش کننده هامعرفی شده اند.

# 2-19 استریم مدیا

حتما می دانید که قرار دادن فایل ها در حافظه گوشی تنها گزینه نیست.چون گوشی های هوشمند اندروید با DATA PLAN هایی فروخته می شوند،امکان اتصال در هر جایی ممکن است،حتما که نباید فایل ها در درون گوشی باشند!

سرویس های قدیمی و البته امتحان پس داده مانند RHAPSODY و PANDORA وجود دارندکه در کار استریم مدیا به کمک آن ها می آیند. یکی از ستاره های دنیای استریم که روز به روز درخشان تر می شود SPOTIFY،نام دارد که به کاربران اجازه استریم کردن مدیا را بر روی گوشی می دهد که سپس کاربر می تواند آن ها با گوشی های دیگر همگام سازی کند. رقیب این ستاره GOOGLE MUSIC BETA ، نام دارد که عملکردی شبیه SPOTFIY را دارد.اگر بخواهیم پارا از این فراتربگذاریم ،به AMAZON MP3 می رسیم که قابلیت استریم مدیا را از درایو ابری آمازون ،یکی از ویژگی های جذاب آن است. همچنین این برنامه به فروشگاه AMAZON MP3 هم متصل است.

استریم ویدئو نیز در این بین چشمک می زند NETFLIX هم اکنون بر روی طیف گسترده ای از گوشی های اندرویدی وجود دارد که به کاربر اجازه اتصال به سرویس عضویت شرکت مربوطه را می دهد.از سایر بازیکنان این زمین می توان به VEVO و PANDORA TV اشاره کردکه برموزیک ویدئو تمرکز کرده اند. حتی خود آندرویت مارکت به کاربران ویدئو هایی را پیشنهاد می دهد که البته باید برای آن ها مبلغی بپردازید. این قابلیت برای گوشی های با ورژن اندروید 1.2 به بالا در دسترس است.

# 2-20 دست دوستی با ITUNES

انتخاب های زیادی در رابطه با نرم افزار های مدیریت مدیا بر روی کامپیوتر های شخصی وجود دارد و البته این قضیه در مورد مک هم صادق است ،اما متداول ترین ومعروف ترین گزینه است که کاربران اندروید را نگران کرده است! درست حدس زده اید .منظورم ITUNES است.

استفاده از ITUNES بر روی دستگاه های اپل کار چندان سختی نیست ،اما قضیه اینجاست که اگر محصولی از شرکت دیگری بخواهد ITUNES را اجرا نماید چه خواهد شد!؟ حقیقت این است که اپل خودش را درگیر این ماجرا نکرده است و اهمیت کمی به این مسئله داده است .حالا،بیشتر خریداران اندروید تصور می کنند دیگر خبری از ITUNES نخواهد بود، اما تصور آن ها صحیح نیست ،چون نرم افزار هایی در دنیای متنوع اندروید زندگی می کنند که می توانند بار دیگر ITUNES را وادار به دادن دست دوستی با شما بکنند!

معروف ترین گزینه برای همگام سازی با ITUNES ، EASY PHONE TUNES است که رایگان بودن آن ،هیچ چیزی از ارزش ها را کم نمی کند!

در طرف مقابل،جایگزین های بسیاری هستند که عملکرد های مشابهی را ارائه میکنند، اما رایگان نیستند.رایگان بودن خوب و البته عالی است، اما دو ویژگی محصولات پولی آن ها را از محصولات رایگان متمایزمی کنند .اول این که ، رابط کاربری بهتری دارند که این ویژگی، همگام سازی ومدیریت کتابخانه با کیفیت تری را به ارمغان می آورد. دیگری این که آنها از همگام سازی WIFI پشتییبانی می کنند. بنابراین برای همگام سازی با ITUNES دیگرنیازی به اتصال فیزیکی با کامپیوتر نخواهید داشت.

در میان محصولات پولی ISYNCER برای خود نامی دست و پا کرده است،چون با وجود ارائه قابلیت WIFI قیمتی بیشتر از 3.98$ و $ 5.99 دارند.

# 2-21 بازارچه اندروید

پیشنهادات و نحوه خرید

همه گوشی های هوشمند اندروید با یک ANDROID MARKETPLACE (همان بازارچه خودمان ) از پیش نصب شده ارائه می شوند.طبق آخرین تغییرات انجام گرفته ،این مارکت نه تنها نرم افزارها را شامل می شود،بلکه این بار با ویدئوها و کتاب ها از شما پذیرایی می کنند!

بیشتر نرم افزار های این مارکت رایگان هستند و به راحتی و فقط با کلیک کردن بر روی دکمه INSTALL در صفحه نرم افزار قابل دانلود شدن هستند.با این حال ،تعدادی از این نرم افزارها نیازمند اطلاعات حساب گوگل را دارند. می توانیدیا از اطلاعات گوگل از پیش ذخیره شده استفاده کنید و یا اطلاعات را بصورت دستی وارد کنید.

زمانی که نرم افزاری را خریدید،دیگر نیازی به خرید مجدد آن برای دستگاه دیگری ندارید،البته تا زمانی که اطلاعات حساب گوگل یکسانی را برای هر دو دستگاه وارد کرده باشید !این نکته بسیار مهم را باید در هنگام مهاجرت به دستگاه دیگری در ذهن نگاه دارید،چون به هر حال با نرم افزارهای بسیاری روبرو خواهید شدکه باید مجددا دانلود و بر روی گوشی جدید نصب کنید.

# 2-22 نرم افزار هدایت گر و به روز رسانی ها

در شرایطی که مارکت به موضوعات مختلفی دسته بندی شده است که همچنین شامل زیر گروه هایی مانند " پر دانلود ترین نرم افزارها "هم هست .البته کار کمی سخت شده است چون هیچ زیر گروه اختصاصی ای وجود ندارد. به طور مثال ،هیچ صفحه اختصاصی برای نرم افزارهای پیام رسان در این مارکت دیده نمی شود.

وقتی نرم افزارها را دانلود کردید،می توانید با وارد شدن به این بازارچه ،نرم افزار های نصب شده را مشاهده کنید.بدین صورت که وارد منو می شوید و سپس بر روی MAY APPS کلیک می کنید.این نرم افزلرها در سه گروه طبقه بندی می شوند:نرم افزارهایی به همراه آپدیت ها،نرم افزارهای نصب شده و نرم افزارهایی که خریداری شده اما هنوزنصب نشده اند. در نظر داشته باشید که نرم افزارهای رایگان حذف شده از گوشی ،هیچ گاه در گروه NOT INSTALLED لیست نمی شوند.

# 2-23 روت کردن اندروید

گوشی های اندرویدی حتی اگر هم دست نخورده باقی بمانند ،قابلیت های زیادی را ارائه می دهند ،امااگر واقعا می خواهید از تمام پتانسیل گوشی استفاده کنید ،باید گوشی را "روت " کنید . "روت کردن "عملی است که درآن سیستم عامل دور زده می شود تا کاربر به تمام امکانات گوشی دسترسی پیدا کند.

فایده روت کردن مشخص است .وقتی گوشی را روت می کنید،گوشی کارایی بیشتری را به دست خواهد آورد.برای مثال بیشتر نرم افزارهای اسکرین شات فقط بر روی گوشی های روت شده اجرا می گردند و البته یک نسخه از این گونه نرم افزارها به نام NO ROOT SCREENSHOT IT وجود داردکه حساسیتی در این باره ندارد،ولی باید برای آن $ 4.99 بپردازید! یکی دیگر از فوایدروت کردن،امکان گرفتن یک آپ کامل از تمام اطلاعات گوشی است. با فوایدی که از روت کردن ذکر شد،با این حال مهم ترین دلیل برای روت کردن CUSOM ROM است، CASTOM ROM نرم افزاری است که از روت کردن ذکر شد، با این حال مهم ترین دلیل برای روت کردن ROM CUSTOM است، ROM CUSTOM نرم افزاری است که می تواند بر روی گوشی اندرویدی شما نصب شود تا سیستم عامل را تغییر دهد .اگرازگوشی ای استفاده می کنید که به هر دلیلی ورژن اندروید آن آپدیت نشده است و قدیمی است،شاید این تنها راه شما برای دسترسی به جدیدترین و بهترین ورژن اندروید باشد .بیشتر ROM ها تغییراتی را در رابط کاربری ایجاد می کنند و دست کاربررا برای اعمال ویرایش های فنی به بخش های مهم گوشی، مثل شماره گیر ،باز می گذارد.

آیا باز هم نمی خواهید روت کنید! بسیار خوب. چون کمی پیچیده به نظر می رسد، در قسمت بعدی باز هم به آن اشاره کرده ایم.اما یکی از نظرات مخالف در مقابل روت کردن ،خطر تبدیل شدن گوشی به یک تیکه آجر را ذکر می کند.نترسید! تنها هنگامی که مراحل روت کردن را به طریقی که گفته شده است ،انجام ندهید ممکن است به فایل های هسته ای سیستم وارد شود که با کمی دقت می توان از آن جلوگیری کرد. توجه داشته باشید که با روت کردن گوشی،در حقیقت برگه گارانتی گوشی را با دست خود پاره خواهید کرد ونباید از سازنده گوشی انتظار خدمات گارانتی را داشته باشید.

# 2-24 چگونه روت کنیم

هیچ راه مشخص و واحدی را برای روت کردن نمی توان ارائه داد ،چون روت کردن گوشی های مختلف به روش های متفاوتی انجام می شود. این بدان معناست که اگر یک روش بر روی یک گوشی مثل EVO 3D به طورمطلوبی جواب داد،نباید حتما از آن انتظار داشته باشیم بر روی MOTORAL DROID هم جواب دهد.

پس کجا باید به دنبال راهنمای روت کردن گوشی خو باشید؟ اساسا دو منبع قابل اعتماد در دسترس هستند. یکی از آن ها ANDROID POLICE است. می توانید سری هم به فروم توسعه دهندگان XDA بزنید که یکی از این فروم ها،فروم جامع هک و نرم افزار اندروید است که می توانید به راحتی راهنمای روت کردن گوشی های جدید را که معمولا پیش ازهر چیز دیگری قرار داده شده اند ،در آن پیدا کنید.

# 2-25 نصب نرم افزارهایی که در مارکت نیستند

گوگل در قرار دادن نرم افزارها بر روی مارکت سخت گیر نیست وبیشتر نرم افزارها بدون جنجال به پا کردن بر روی آن قرار می گیرند. البته این قضیه برای همه نرم افزارها صدق نمی کند. گاهی اوقات اختلاف سلایق باعث می شود یک نرم افزارنتواند از طریق کانال های رسمی و عمومی انتشار پیدا کنند.

نر م افزارهای فروشگاه آمازون و شبیه سازها که به کاربران اجازه ی اجرای بازی های کنسول های قدیمی را بر روی گوشی های اندرویدی می دهند،از این قبیل نرم افزارها هستند. وقتی شرکت سونی SONY XPERIA PLAY را عرضه کرد,تعداد،زیادی از شبیه سازها از مارکت برداشته شدند،چون آن ها رقبای مهمی برای دستگاه سونی به شمار می رفتند.

به هر صورتی که هست ،اگر نرم افزاری در مارکت وجود نداشته باشد،می توان با استفاده از فایل نصاب آن (INSTALLER ) آن را در گوشی نصب کرد که این فایل با فرمت ASK وجود دارد.فایل مورد نظر می تواند با استفاده از خود گوشی دانلود شود.و یا با استفاده از PC دانلود و به گوشی انتقال داده شود.در صورتی که گزینه دوم را انتخاب کنید،همواره به یک نرم افزار مدیریت فایل احتیاج خواهید داشت تا فایل را درون گوشی مستقر کنید که پیدا کردنش هم چندان سخت نیست!

پروسه نصب همانند پروسه دانلود یک نرم افزار سریع و ساده است. فقط تنها مشکلی که وجود دارد این است که گوشی های اندرویدی طوری پیکر بندی شده اند که عملیات نصب یک نرم افزار از یک منبع نامشخص را رد می کنند.بدین صورت که هنگامی که فایل APK را باز می کنید با پیغامی مبنی بربلاک شدن عملیات نصب مواجه خواهید شد.شما می توانید طبق میل خودتان تنظیمات نصب را تغییر دهید.به منو وارد شوید،به بخش تنظیمات رفته و بخش نرم افزارها را انتخاب کنید. در منوی باز شده،اولین گزینه " UNKNOWN SOURCES " )منابع نامشخص )خواهد بود که می توانید آن را تغییر دهید تا دیگر مشکلی از این بابت نداشته باشید.

# 2-26 شخصی سازی آهنگ های زنگ و پیام

مثل بقیه گوشی ها، آهنگ های زنگ وپیام های گوشی های اندرویدی هم میتوانند بر اساس میل شما تنظیم شوند.اگر به دنبال راهی آسان و ساده برای شخصی سازی هستید،دانلود یک نرم افزار برای به اشتراک گذاری رینگتون ها کافی به نظر می رسد. نرم افزار مورد علاقه من ZEDGE است،اما گزینه های متعدد دیگری هم در مارکت وجود دارند. راحت باشید و به چشم رایگان به آن ها نگاه کنید!

کاربرانی که آپشن های بیشتری می خواهند، باید دنبال نرم افزار هایی بگردند که به آن ها اجازه می دهد تا رینگتون های شان را کات کنند. دوباره تکرار میکنم نرم افزار های متعددی در این زمینه ها وجود دارند، اما من از RINGTONE MAKER (MOBILE 17 ) استفاده میکنم.

این نرم افزار به کاربران اجازه می دهد تا قسمتی از یک فایل صوتی را کات کنند و فایل حاصله را به عنوان رینگتون استفاده کنند. این نرم افزار همچنین می تواند پیشنهاداتی در مورد چگونگی کات کردن فایل شما – بر اساس فایل های آپلود شده دیگر کاربران – بدهد.

وقتی که کارتان را با نرم افزار انجام دادید ، می توانید بلافاصله یک پیش نمایش از فایل حاصله را بشنوید تا ببینید چه چیزی از آب درآمده است! به همین سادگی وخوشمزگی!

# 2-27 امنیت و اهمیت دسترسی ها

به وجود آوردن شرایطی برای نرم افزار ها که از طریق آن بتوانند توسعه پیدا کنند و بر روی مارکت آپلود شوند ، نباید از امنیت بوی نبرده باشد و این هم دلیلی است بر داغ بودن مبحث امنیت سیستم عامل های موبایل ! گوشی های هوشمند ، شامل اطلاعات زیادی از قبیل مخاطبان ، آ شنایان و کسانی که با آن ها در تماس هستیم را شامل می شوند.حتی هر کجا می رویم رد پایی به جای می گذاریم که این گو شی های هوشمند ، همانطور که از اسمشان پیداست ،اطلاعات را ضبط و نگهداری می کنند. آن ها هم چنین پا را فراتر گذاشته اند و اطلاعا ت کارت اعتباری را دارا و همینطور به حساب بانک ما دسترسی دارند.

توجه به دسترسی هایی که ما به گو شی می دهیم ، اهمیت فوق العاده ای دارد. اولین خط از انشای امنیت ، در هنگام نصب یک نرم افزار ، پرسیدن این سوال از خود است : " آیا این نرم افزار برای دسترسی به اطلاعات مهم گوشی اجازه می خواهد ؟ " به طور مثال ، یک LIVE WALLPAPER که برای دسترسی به اطلاعات مکان فعلی شما،اجازه می خواهد مطمئنا خوشاین به نظر نمی رسد!

# 2-28 ابراز مبارزه با MALWARE ها – دفاع غیر عامل

اجازه برای دسترسی ها ، امکان دسترسی نرم افزار ها را به ا طلاعات مهم گوشی چک می کنند . در واقعیت ، در هنگام نصب نرم افزار ، کار بر وقت آن چنان زیادی برای فکر کردن به این موضوع صرف نمی کند و احتمالا به هر نحوی آن را تایید می کند . در نهایت ، بهتر است از روش های غیر عامل برای شناسایی و برخورد با MALWARE ها استفاده کنید.

از این لحاظ ،مارکت اندروید رو سفید است و کمبودی از بابت نرم ازارهای امنیتی ندارد.نرم افزاری مانند FREE ANTE- VERUSVS که توسط شرکت AVG ساخته شده است،گزینه خوبی است.

آنتی مالورها همان اندازه که به فکر امنیت یک کامپیوتر معمولی اند،به فکر اندروید هم هستند واز هیچ کاری کم نمی گذارند . این طور نیست که فکر کنید چون در دنیایی به مراتب کوچکتر کار می کند،پس کمبودهایی هم خواهد داشت. نه ! هر کاری از دستش بر می آید! این همونه ،فقط ابعادش عوض شده !

نرم افزارها بعد از دانلود شدن توسط این نرم افزارها اسکن می شوند و با یک بانک اطلاعاتی از تحدید های بروز چک می شوند.به علاوه ،بعضی از این نرم افزارها ی امنیتی ،به طور همیشگی درحال اسکن هستند و ه دنبال حرکت مشکوکی از جانب نرم افزارها خواهند بود!

# 2-29 مانیتورینگ گوشی

در این شکی نیست که نرم افزارهای آنتی مالور از گوشی شما محافظت می کند ،اما هیچ ضمانتی منوط به شناختن همه تحدید ها ،مخصوصا جدیدهایشان ،در کار نیست.درست مانند PC ها ،متاسفانه، مالورها می توانند از طریق اینترنت گوشی،اطلاعات را به منبع دیگر یا شخص دیگری ارسال کنند،اما گوشی های هوشمند خوشبختانه نمی توانند از حد معینی در ماه ،بیشتر،اطلاعات دریافت/ارسال کنند.بنابراین مانیتورینگ کار خیلی سختی نخواهد بود!من شخصا از نرم افزار TRAFFEC MONITOR استفاده می کنم که حجم ارسال و دریافت اطلاعات نرم افزار ها را کاهش می دهد و حتی می تواند در صورت نیاز ،نرم افزاری را بلاک کند.همیشه سوء استفاده از اطلاعات گوشی ،هدف بدافزارها نیست. به طور مثال،یک تروجان که به گوشی های اندروید روسیه حمله کرد،برنامهاش ارسال اس ام اس به یک شماره خاص و دریافت اعتبار ازگوشی بود.استفاده از برنامه ای مثل PHONE USAGE که از بخش دریافت و ارسال اس ام اس چشم بر نمی دارد،می تواند در این گونه شرایط مفید واقع شود.

# 2-30 امنیت فیزیکی

خیلی از کاربران نگران دسترسی بد افزارها به گوشی و دزدیدن اطلاعات هستند،در حالی که اکثر اوقات همین کاربران ،از امنیت دسترسی فیزیکی به گوشی شان غافل می شوند . مطمئنا گم شدن گوشی ،کاربر را به مراتب بیشتر از نفوذ یک بد افزار ،تحدید می کند. مواظبش باشید !

اولین قدم ،قفل کردن گوشی است .اگر حالا که دارید این کلمات را می خوانید ،گوشی تان از یک قفل اتوماتیک برخوردارنیست،بپرید و یک تنظیم قفل برای گوشی تان ردیف کنید! برای این کار وارد منو شوید ،به قسمت تنظیمات رفته و سپس بخش امنیت را باز کنید.این قسمت ،گزینه " CHANGE SCREEN LOCK " را انتخاب کنید.با این کار سه آپشن در روبروی شما خواهد بود: استفاده از یک الگو،کد پین و یا رمز.

بله ! این یعنی وقتی می خواهید از گوشی استفاده کنید حتما باید کدی را وارد کنید! قبول دارم که گاها اعصاب خوردکن می شود، اما وقتی که گوشی تان دست یک آدم بوق افتاد ضایع خواهد شد!

# 2-31 دلایل برتری گوشی های اندروید در مقایسه با آیفون

زمانی که اندروید با گوشی رویایی HTC (نکسیوس وان گوگل ) در مهر88 آغاز به کار کرد این گوشی IPHONE KILLER نام گذاری شد.اگر چه این گوشی نتوانست به کلی آیفون را نابود کند اما این اولین قدم یک انقلاب بر ضد آیفون بود.پلتفرم اولیه اندروید در چندین مرحله حتی جای IPHONE OS رانیز گرفت،اما اندروید یک سری از کارایی های کلیدی که آیفون می توانست فراهم کند را کم داشت. بعد از این اتفاق،اندروید رشد کرد ،نه در زمینه کارایی هایی مشابه آیفون ،بلکه بهترین مورد رشد اندروید وجود گوشی های مختلف اندرویدی در فروشگاه ها می باشد که نشان ازموفق بودن این پلتفرم می دهد. آیفون هم اکنون با فقط یک گوشی یا یک برند رقابت نمی کند، بلکه با پلتفرمی رقابت می کند که هزاران تلفن همراه را به بازار روانه خواهد کرد.

# شکل 2- 1 مقایسه آیفون و اندروید



# 2-32 آینده اندروید

مسلما تب اندروید به این زودی فروکش نخواهد کرد. هجوم بی سابقه شرکت ها برای تولید محصولات مبتنی بر اندروید رفته رفته طیف گسترده تری ازمحصولات شامل تلفن همراه ،تلوزیون ،نت بوک و تبلت را در می گیرد.به نظر می رسد همه چیز به کام اندروید است و به سختی می توان تصور کرد سیطره این پدیده به سادگی قابل شکستن باشد.آدم آهنی بازیگوش سبز رنگ ما در مدت زمان کوتاهی که از تولدش می گذرد،نشان داده هر روز به دنبال غافلگیر کردن ما و سرک کشیدن به یکی دیگر از وسایل الکترونیکی ماست تا آن را نیز جولانگاه شیطنت های دوست داشتنی خود نماید.

# 2-33 اندروید و گوگل تی وی

خوب اگر فکر کرده اید که کار شما با اندروید تمام شده است سخت در اشتباه هستید. اگر کار شما هم با اندروید تمام شده باشد، کار اندروید با شما تمام نشده است . بلکه این آدم آهنی سبز رنگ پس از رسوخ در تلفن های همراه شما قصد دارد وارد تلوزیون های شما هم بشود. به چشمان خود شک نکنید . درست خوانده اید اندروید به زودی در تلوزیون های شما نیز خواهد بود. در همایش Google i/o در ماه مه 2010 شرکت های گوگل ،سونی ،اینتل ،لاجیتیک ،بست بای ،ادوبی و دیش نتورک از عرضه تلوزیون های مبتنی بر اندروید خبر دادند.

تلویزون هایی که به طور بی سیم به اینترنت متصل می شوند و علاوه بر اینکه امکان اتصال به شبکه های آنلاین پخش فیلم رادارند، از برنامه های کاربردی که برای نصب بر روی این تلوزیون ها تهیه می شوند نیز بهره خواهند برد.

# فصل سوم

# امنیت در اندروید

# مقدمه

رشد سریع گوشی های هوشمند منجر به یک رنسانس در سرویس های موبایل شده است , برنامه های قابل استفاده در هرجا یک ارایه وسیع خدمات اجتماعی , مالی و سرمایه گذاری را برای هرکاربر با طرح داده ی سلولی , پشتیبانی می کند . بازار های برنامه مانند فروشگاه برنامه های اپل و بازار اندروید گوگل نقطه ای برای دستیابی کلیکی برای صد ها یا هزاران برنامه ی رایگان و پولی فراهم می کنند. بازار های ساده بازاریابی نرم افزار , نصب , و بروز رسانی - موانع کمی برای اوردن برنامه ها به بازار , و حتی موانع کمتر ی برای کاربران دستیابی و استفاده از ان در ان ایجاد شده است.

فعالیت بازارها نیز چالش های امنیتی بسیار زیادی ارایه می کنند . توسعه و گسترش سریع برنامه ها , سیستم های مجوز بزرگ , رفتار های حمله امنیتی , بدافزار ها , و مدل های امنیتی محدود منجر به داشتن تلفن ها و برنامه های اسیب پذیر شده است. اگرچه کاربران به ظاهر به ان اعتماد دارند , بازارها در موقعیت فراهم کردن امنیت در بیشتر از یک روش سطحی نیستند. فقدان یک تعریف رایج برای امنیت و حجم برنامه ها تضمین می کند که برخی برنامه های مخرب , مشکوک , برنامه های اسیب پذیر راه خود را در این بازار پیدا کنند.

که یک مکمل دیکامپایلر ded دالویک , طراحی شده است. ded یک منبع جاوا فقط برنامه از نسخه نصبی به وسیله ی با استنتاج از انواع از بین رفته , انجام بازیابی بایت کدهای DVM از JVM , و ترجمه ی کلاس ها و ساختار متد ها , باز می گرداند.

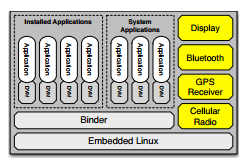
۲۱ میلیون LOC بازیابی شده رو از ۱۱۰۰ برنامه رایگان در بازار اندروید به وسیله ی ازمایشات خودکار و بررسی کتابچه راهنمای کاربر , تجزیه و تحلیل کردیم. که قدر شناسایی دلایل اصلی و فرض شدت اسیب های کشف شده , ساخت. تجزیه و تحلیل امنیتی متمرکز بر محبوبیت ما بینشی بر برنامه های با بیشترین استفاده فراهم کرد. یافته ها طبق مشاهدات زیر شکل گرفتند.

1. مشابه با مطالعات قبلی سواستفاده های بسیاری از اطلاعات حساس امنیتی- شناسه های گوشی های خاص و موقعیت جغرافیایی - یافتیم. شناسه های گوشی مانند IMEI , IMSI و ICC-ID , همه چیز از ردیابی "کوکی اسکو" تا شماره حساب ها استفاده می شود.
2. هیچ مانعی برای سواستفاده های تلفنی , ضبط ویدیو و صوت در پس زمینه , ارتباطات سودجویانه , یا لیست برداری از برنامه های نصب شده وجود ندارد .
3. کتابخانه های شبکه های تحلیلی و تبلیغاتی با ۵۱ درصد از برنامه های مطالعه شده , با تبلیغات مخرب (آشکار شده در ۲۹.۰۹ درصد برنامه ها) , و تبلیغات گوگل (آشکار شده در ۱۸.۷۲ درصد از برنامه ها ) در این بازی در ارتباط اند. بسیاری از برنامه ها شامل بیش از یک کتابخانه تبلیغاتی هستند.
4. بسیاری از تپسعه دهندگان در استفاده امن از API های اندروید دچار شکست می شوند. این شکست ها به طور کلی درون طبقه بندی محافظت ناکافی از اطلاعات حساس امنیتی اتفاق می افتند. به هر حال هیچ بهره برداری آسیب پذیری که بتواند کنترل مخرب گوشی رو منجر شود , وجود ندارد.

اندروید: اندروید یک سیستم عامل طراحی شده برای گوشی های هوشمند است. در شکل یک نشان داده شده است , اندروید یک جعبه ایمن محیط اجرای برنامه های کاربردی را فراهم می کند. یک سیستم لینوکس سفارشی تعبیه شده با سخت افزار گوشی و یک پردازنده ی رادیوی سلولی در تعامل است. میان افزار الحاق و API های برنامه ها در بالای لینوکس اجرا می شود. برای ساده سازی برنامه کاربردی تنها رابط گوشی از طریق این API ها است. هر برنامه درون یک ماشین مجازی دالویک (DVM) اجراشده تحت uid منحصر به فرد یونیکس , اجرا می شود. گوشی پیش نصب شده با یک انتخاب از برنامه های سیستم , مانند , شماره گیر تلفن , دفترچه ادرس , به بازار می اید.

برنامه های کاربردی با یکدیگر و تلفن از طریق اشکال مختلف IPC تعامل می کنند. مفاد , مفاد , پیام های درون پردازنده تایپ شده ای هستند که به برنامه های کاربردی خاص یا سرویس های سیستم جهت می دهند , یا پخش جمعی برای برنامه های کاربردی که به منظور خاصی تعریف شده اند , انجام می شود. فراهم کننده ی محتوای مداوم مخازن داده از طریق رابط شبیه به sql جستجو می شوند. خدمات پس زمینه رابط های RPC و پاسخ تماس که برنامه های مورد استفاده در فعالیت های تریگر یا دستیابی به داده هستند را فراهم می کند. سر انجام رابط فعالیت های کاربر سیگنال های فعالیت نامداری داری از سیستم و دیگر برنامه های کاربردی دریافت می کند.

فعالیت های الحاقگر به عنوان یک نقطه میانی برای همه ی IPC ها است. دستیابی به منابع سیستم (مانند گیرنده های GPS , پیام رسانی متنی , سرویس های تلفن , و اینترنت) , داده ها ( مانند دفترچه تلفن و ایمیل) و IPC ها توسط مجوز های دسترسی طراحی شده در زمان نصب اختیاردهی می شوند. مجوز ها توسط برنامه های کاربردی درخواست می شوند و مجوز های مورد نیاز برای دستیابی برنامه کاربردی به رابط یا داده در فایل بیانیه تعریف می شوند. به بیان ساده , یک برنامه کاربردی اجازه ی دستیابی یک منبع یا رابط را دارد , اگر مجوزهای مورد نیاز به ان امکان دهند. انتصاب مجوز - و مجوز های غیر مستقیم امنیت برای تلفن- تا حد زیادی به مالک تلفن واگذار می شود. کاربر یک لیست مجوز های درخواستی برنامه را در زمان نصب مشاهده می کند , که می تواند قبول یا رد کند.



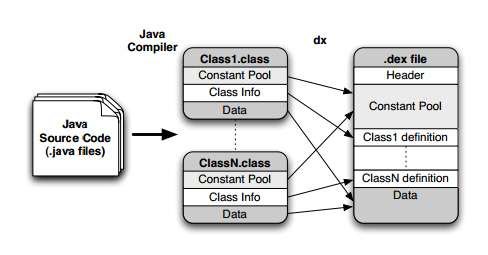
# شکل 3- 1معماری سیستم اندروید

ماشین مجازی دالویک: برنامه های کاربردی در جاوا نوشته می شوند , اما در DVM اجرا می شوند. DVM ومحیط زمان اجرای بایت کد های جاوا به طور قابل ملاحظه ای متفاوتند：

ساختار برنامه: برنامه های جاوا از یک یا چند فایل کلاس تشکیل شده اند , یک فایل در هر کلاس. JVM بایت کدهای یک کلاس جاوا از فایل کلاس مربوطه را که درزمان اجرا ارجاع داده شده است بارگیری می کند. برعکس یک برنامه دالویک از یک فایل .DEX شامل همه ی کلاس های برنامه تشکیل شده است.

شکل ۲ یک دید مفهومی از فرایند کامپایل برنامه های DVM فراهم می کند. بعد از اینکه کامپایلر جاوا بایت کد های JVM را ساخت , کامپایلر DX دالویک , کلاس فایل ها را مصرف می کند و انها را به بایت کدهای دالویک دوباره کامپایل می کند, ونتایج برنامه را در یک فایل .DEX تنها می نویسد.این فرایند شامل ترجمه , بازسازی و تفسیر سه عنصر اصلی برنامه ： دسته های ثابت , تعریف های کلاس ها , قسمت داده می باشد. جای تعجب نیست که دسته های ثابت های مورد استفاده در کلاس ها را تعریف می کند. این شامل, در میان دیگر موارد , ارجاعات به دیگر کلاس ها , اسامی متد ها و ثابت های عددی است. تعریفات کلاس ها از اطلاعات اصلی مانند فلاگ های دستیابی و نام های کلاس ها تشکیل شده است. عناصر داده شامل کد متد اجرا شده در ماشین مجازی مقصد و همچنین دیگر اطلاعات مرتبط با روش ها (مانند تعداد ثبات های DVM استفاده شده , جدول متغیر محلی , و اندازه عملگر پشته) و کلاس ها و نمونه های متغیر ها است.

معماری ثبات : DVM ثبات محور است درحالیکه JVM های موجود پشته محور هستند. بایت کدهای جاوا میتوانند متغیر های محلی را برای یک.جدول متغیر محلی قبل از قرار دادن انها درون یک عملگر پشته برای محاسبه توسط اپ کدها انتصاب کند , اما همچنین می تواند فقط بر روی پشته بدون ذخیره سازی صریح متغیرها در جدول کار کند. بایت کد های دالویک متغیر های محلی را برای هر یک از ۲ به توان ۱۶ ثبات در دسترس انتصاب می کند. اپ کد های دالویک به جای دستیابی به عناصر بر روی پشته ی یک برنامه , مستقیما ثبات ها را دستکاری می کنند.



# شکل 3- 2 فرایند کامپایل برنامه های DVM

مجموعه ی دستورالعمل ها. مجموعه دستورالعمل های بایت کد دالویک تفاوت قابل توجهی با ان در جاوا دارد. دالویک ۲۱۸ اپ کد دارد درحالیکه جاوا ۲۰۰ تا. با این حال طبیعت اپ کد ها خیلی متفاوت است. برای مثال جاوا ده اپ کد مشخص شده برای جابجایی عناصر بین پشته و جدول متغیر های محلی دارد ؛ دستورالعمل های دالویک گرایش به طولانی تر بودن از دستورالعمل های جاوا دارند؛ انها اغلب شامل ثبات های منبع و مقصد هستند . در نتیجه برنامه های دالویک دستورالعمل های کمتری نیاز دارند. در بایت کد دالویک , برنامه ها میانگین ۳۰ % دستورالعمل های کمتری نسبت به جاوا دارند , اما ۳۵ % اندازه کد بیشتر(بایت).

ساختار دسته ثابت . برنامه های کاربردی جاوا عناصر دسته های ثابت را درون فایل های کلاس چند گانه تکرار می کنند مانند نام روش های ارجاع گیرنده و ارجاع کننده. علاوه بر این dx برخی ثابت ها را به وسیله ی جاگذاری مستقیم مقدارها درون بایت کد ها خذف می کند. در عمل عناصر اینتیجر , لانگ اینتیجر , عناصر میمیز شناور سینگل و دابل , در طی این فرایند محو می شود.

ساختار کنترل جریان. عناصر کنترل جریان مانند حلقه ها عبارات انتخابی , و مدیریت استثنا به طور متفاوت در دالویک و بایت کد جاوا ساخته شده اند. ساختار بایت کد جاوا ازادانه کد منبع را قرینه می کند درحالیکه بایت کد دالویک نه.

انواع مبهم پیشین . متغیر بایت کد جاوا انتصاب بین ثابت های اینتیجر (int) و ممیز شناور سینگل (float) و بین ثابت های لانگ اینتیجر(long) و ممیز شناپر دابل (double) را انجام می دهند. با این حال انتصاب دالویک (int/float و long/ double) از اپ کد های یکسانی برای اینتیجر و فلوتس وغیر استفاده می کند. اپ کد ها اعشار ویژه گذشته بی نوع هستند.

ارجاع تهی . بایت کد های دالویک یک نوع تهی مشخص نمی کند به جای ان از یک مقدار ثابت صفر بهره می جوید. بنابراین مقادیر ثابت صفر ارایه شده در بایت کدهای دالویک نوع مبهمی دارد که نیاز به بازیابی دارد.

مقایسه ی اشیا ارجاع. بایت کدهای جاوا از اپ کدهای نوع دار برای مقایسه ی اشیا ارجاع (if\_acmpeq و if\_acmpne) و برای مقایسه تهی بودن اشیا ارجاع (ifnull , ifnonnull) استفاده می کند. بایت کدهای دالویک از مقایسه ی اینتیجر ساده تری برای این اهداف استفاده می مند ؛ به ترتیب یک مقایسه بین دو اینتیجر و مقایسه یک اینتیجر و صفر . این به فرایند دیکامپایل برای بازیابی انواع برای مقایسه ی اینتیجر استفاده شده در بایت مد DVM نیازمند است.

ذخیره ی انواع پیشین در ارایه ها. بایت کد های دالویک از اپ کد های مبهم برای ذخیره و بازیابی عناصر در ارایه های انواع پیشین ( مانند aget برای int/float و aget\_wide برای long/double ) استفاده می کند در حالیکه بایت کد متناظر جاوا غیر مبهم است. نوع ارایه باید برای ترجمه صحیح بازیابی شود.

# 3-1 دیکامپایلر ded

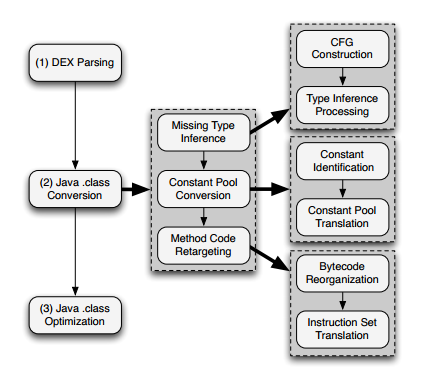
ساختن یک دیکامپایلر از dex به جاوا برای این مطالعه با چالش های تعجب اوری روبرو شد. از یک طرف دیکامپایل کردن جاوا از سال ۱۹۹۰ مطالعه شد - ابزار هایی مانند موچا برگشت به یک دهه قبل , با بسیاری از تکنیک های در حال توسعه دیگر. متاسفانه قبل از کار ما هیچ ابزار تابعی برای بایت کد دالویک وجود نداشت. به دلیل اینکه تفاوتهای گسترده ای بین JVM , DVM وجود دارد , تغییر اسان دیکامپایلر موجود امکان پذیر نبود.

این انتخاب برای دیکامپایل منابع جاوا به جای عملیات مستقیم بر روی اپ کدهای dex به دو دلیل بنا نهاده شد. اولا ابزارهای موجود برای تجزیه و تحلیل کد را بررسی کنیم. دوما ما نیاز به دستیابی به کد های منبع برای شناسایی مزایای غلط حاصل از تجزیه و تحلیل خودکار کد را , مانند انجام تایید دستی , شناسایی کنیم.

استخراج ded در سه مرحله اتفاق می افتد： الف. بازیابی , ب. بهینه سازی , ج. دیکامپایل کردن. این قسمت چالش ها و فرایند ded را نشان می دهد و با خلاصه ای از بحث اعتبار سنجی اش نتیجه گیری می شود.برای خوانندگان علاقه من منبع برای یک مطالعه ی کلی معرفی شده است.

# 3-2 بازگردانی برنامه

مرحله ی اول دیکامپایل کردن بازگردانی فایل .dex برنامه به کلاس های جاوا است. شکل ۳ این فرایند را مرور می کند ： ۱.بازیابی اطلاعات نوع , ۲. ترجمه دسته های ثابت و ۳. بازگردانی بایت کد.



# شکل 3- 3بازگردانی بایت کد دالویک

استنتاج نوع ： مرحله ی اول بازگردانی شناسایی متد ها و کلای های ثابت و متغیر است.هرچند بایت کد دالویک همیشه اطلاعات کافی برای تعیین نوع یک متغیر یا ثابت از اعلانات ثبات هایش فراهم نمی کند. دو مورد در جاییکه نوع متغیر مبهم است تعمیم داده شده است ： ۱. اعلان متغیر یا ثابت فقط عرض متغیر را مشخص می کند ( مانند ۳۲ یا ۶۴ بیت ) اما مشخص نمی کند فلوت , اینتیجر , یا ارجاع تهی است؛ و ۲. عملگرهای مقایسه بین اینتیجر و مقایسه اشیا ارجاع انجام نشده است.(مانند بررسی ارجاع تهی).

استنتاج نوع به شکل گسترده مورد مطالعه قرار گرفته است. الگوریتم اولیه ی هیندلی میلنر اساس الگوریتم های استنتاج نوع که توسط بسیاری از زبان ها مانند هاسکل و ام ال استفاده شده است را فراهم می کند. این روش ها انواع ناشناخته را به وسیله ی مشاهده ی اینکه چگونه متغیر ها در عملیات با عملوند های شناخته شده استفاده می شوند , تعیین می کند. تکنیک های مشابهی نیز توسط زبان هایی با استنتاج نوع قوی مانند OCAML و همچنین ارجاع ضعیف تر مانند PERL استفاده شده است.

ا.ded روش های مورد قبول را تطبیق می دهد ： اثبات انواع ثبات به وسیله ی مشاهده ی اینکه انها در عملیات بعدی با عملوند های شناخته شده چگونه استفاده شده اند. ثبات های دالویک ازادانه با متغیر های جاوا تطبیق داده می شوند. زیرا بایت کد دالویک ثبات هایی که در حوزه طولانی تر نیستند را دوباره استفاده می کند, ما باید نوع ثبات درون متن متد کنترل جریان اش را ارزیابی کنیم, به عبارت دیگر استنتاج باید حساس به مسیر باشد.بیشتر توجه داشته باشید که استنتاج نوع همچنین متدمحلی است. زیرا انواع پارامتر های ارسالی و مقادیر بازگشتی توسط علایم متد ها شناسایی می شود. نیازی به جستجو خارج از متد نیست.

سه روش ded برای استنباط نوع ثبات وجود دارد. اول هر مقایسه ی ثابت یا متغیر نوع شناخته شده ی در معرض نوع. مقایسه ی انواع نامشابه نیازمند نوع اجباری در جاوا دارد , که در بایت کد دالویک اورده شده است. از این رپ مقایسه ی قانونی دالویک همیشه شامل ثبات های با نوع یکسان است. دوم دستورالعمل هایی مانند add-int فقط بر نوع خاصی عمل می کنند , اشکارا در معرض اطلاعات نوع . سوم دستورالعمل هایی که ثبات ها را به متد ها می فرستند یا از یک مقدار بازگشتی استفاده می کنند , در معرض نوع از طریق علامت متد قرار می گیرند.

الگوریتم استنتاج نوع ded شرح زیر است ：

بعد از بازسازی گراف کنترل جریان , ded همه اعلانات ثبات مبهم را شناسایی می کند. برای هر نمونه ثبات دستورالعمل ها در گراف کنترل جریان را با شروع از اعلانش می پیماید . هر شاخه از کنترل جریان رویت شده درون یک پشته ی استنتاج قرارمیگیرد(push) , مثلا ded یک جستجوی اول عمق بر روی گراف کنترل جریان به دنبال نوع مقابل دستورالعمل ها انجام می دهد. اگر نوع مقابل دستورالعمل رویت شد, متغیر برچسب خورده و فرایند برای این متغیر به پایان می رسد.

سه رویداد وجود دارد که منجر به تمام شدن جستجوی شاخه می شوند ： الف. زمانی که ثبات به متغیر دیگری انتساب داده شده باشد(یعنی یک الان جدید رویت شده است) , ب. زمانی که یک تابع بازگشتی رویت شود , و ج. زمانی که یک استثنا اتفاق بیافتد. پس از اینکه یک شاخه رها شد , شاخه ی بعدی از پشته برداشته شده و جستجو ادامه پیدا می کند. در اخر اطلاعات نوع به جلو منتشر می شود , ثبات پیمانه, از طریق گراف کنترل جریان از هر اعلان ثبات تا همه ی کاربرد های مبهم بعدی , دوباره انتساب می شود. این الگوریتم همه ی نوع های مبهم قبلی را حل می کند , به جز بزای یک مورد مجزا , زمانی که همه ی مسیر های منتهی به یک نوع سرچشمه دستورالعمل مبهم با ستورالعمل ثابت مبهم است .(مانند همه مسیر های منتهی به یک سرچشمه مقایسه ی اینتیجر با ثبات های مقدار گرفته از یک ثابت صفر) . در این مورد , نوع در دیکامپایل کردن تاثیر نمیگیرد و یم نوع پیش فرض (مثلا اینتیجر) می تواند انتساب داده شود.

تبدیل دسته ثابت ： دسته های ثابت .dex و .class به این گونه متفاوتند ： الف. دالویک یک دسته ی ثابت تنها برنامه کاربردی نگهداری می کند و جاوا برای هر کلاس یکی و ب. بایت کد دالویک ثابت های نوع پیشین را مستقیما در بایت کد جای می دهد در حالیکه جاوا از دسته ی ثبات برای بیشتر ارجاعات استفاده میکند. ما اطلاعات دسته ی ثابت را در دو مرحله تبدیل می کنیم.

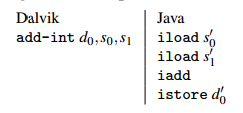
اولین مرحله شناسایی ثابت های است که برای یک فایل کلاس مورد نیاز است. ثابت ها شامل ارجاعات به کلاس ها , متد ها و نمونه های متغیر ها می باشند. Ded بایت کد را برای هر متد در یک کلاس با توجه به ارجاعات پیمایش می کند. ded همچنین همه ی ثبات های پیشین را شناسایی می کند.

وقتی ded ثابت های مورد نیاز را به وسیله ی یک کلاس شناسایی می کند. ان را به فایل class. مقصد اضافه می کند. برای ثابت های نوع پیشین مکان های جدید ایجاد می کند. برای کلاس , متد , نمونه متغیر های ارجاعات , مکان ها ی دسته ثابت های جاوا ایجاد شده بر مبنای مکان های دسته ثابت دالویک هستند. قالب دسته ی ثابت در پیچیدگی متفاوت است.به شکل خاصی مکان های دسته ثابت دالویک به شکل قابل توجهی از ارجاعات بیشتری برای کاهش سربار حافظه استفاده می کند.

بازگردانی کد متد ： مرحله ی نهایی فرایند بازگردانی ترجمه کد متد هاست. اول ما بر روی بایت کد برای شناختن ساختار هایی که نمی توانند به طور مستقیم بازگردانی شوند , پیش پردازش انجام می دهیم. سپس به طور خطی بایت کد DVM را پیمایش پ به JVM ترجمه می کنیم.

ترجمه بایت کد به شکل خطی بر روی هر دستورالعمل دالویک پردازش انجام می دهد.اولا نقشه های ded هر ثبات را به یک شاخص جدول متغیر محلی جاوا ارجاع می دهد. دوم ded یک دستورالعمل ترجمه برای هر دستورالعمل دالویک رویت شده انجام می دهد. همچین بایت مد دالویک و تراکم بیشتر و وظایف ارگومان های بیشتر دارند , یک دستورالعمل دالویک برای دستورالعمل های چند گانه جاوا پر تکرار گسترش می یابد. سوم ded افست های مرتبط استفاده شده برای شاخه ها برمبنای پردازش حاشیه نویسی بهم وصل می کند. سرانجام ded جدول استثنا ها را بلوک های try/catch/finally توصیف می کند , تعریف می کند. کد ترجمه شده ی حاصل با دسته های ثابت برای یک فایل جاوا class. قانونی ترکیب می کند.

در زیر یک مثال ترجمه برای add-int امده است ：

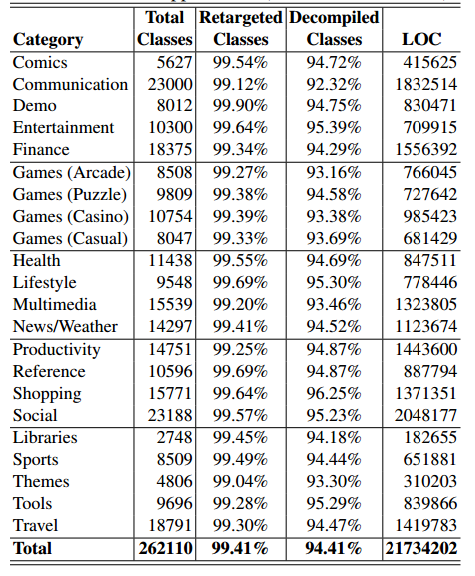


که ded یک متغیر محلی جاوا برای هر ثبات مانند ........ وغیره ایجاد می کند.ترجمه ۴ دستورالعمل جاوا ایجاد می کند ： دوتا برای قرار دادن متغیر در پشته یکی برای جمع و یکی برای برداشتن نتیجه.

# 3-3 بهینه سازی و دیکامپایل کردن

در این مرحله فایل های class. بازگردانی شده می توانند با استفاده از ابزار های موجود مانند فرن فلاور یا سووت , دیکامپایل شوند . با این حال فرایند ترجمه بایت کدهای ded کد جاوا بهینه نشده بدست می دهد. برای مثال ابزار جاوا اغلب انتصاب های غیر ضروری به جدول متغیر های محلی را بهینه می کنند , مانند مقادیر بازگشتی بی نیاز . بدون بهینه سازی کد دیکامپایل شده پیچیده و تجزیه و تحلیل بی نتیجه خواهد شد. علاوه بر این محصولات مصنوعی فرایند بازگردانی می توانند منجر به خطای دیکامپایل سازی در برخی دیکامپایلر ها شوند . نیاز به بهینه سازی بایت کد به اسانی با توجه به حلقه های دیکامپایل شده نشان داده می شود. اغلب دیکامپایلر ها حلقه های for را به حلقه های بی پایان با دستورالعمل break تبدیل می کنند. در حالی که سورس کد حاصل به شکل تابعی برابر با نسخه اصلی است , این به طور قابل توجهی برای تجزیه و تحلیل و درک سخت تر است , به ویژه برای حلقه های تودرتو.بنابراین ما از سووت به عنوان یک بهینه ساز پیش بازگردانی استفاده می کنیم. در حالی که سووت در اصل یک ابزار بهینه سازی در اغلب موارد با توانایی بازیابی سورس کد است , این اصطلاحات برنامه ی قانونی اصلی (ساختار بایت کد) تولید شده توسط ded را پردازش نمی کند. ما به طور خاص دو برنامه مرکزی را مورد بررسی قرار دادیم شامل ۱. تعاملات بین بلاک های همگن و مدیریت استثنا ها , و ۲. کنترل جریان پیچیده به دلیل عبارات break . در حالی که بایت کدهای جاوا تولید شده توسط ded قانونی هستند , نرخ شکست سورس کد گزارش شده در قسمت بعد به دلیل ناتوانی سووت در استخراج سورس کد از این دو مورد تقریبا کامل است. ما دیگر دیکامپایلر ها را در کارهای اینده مانند جدJD و فرن فلاور ، در نظر خواهیم گرفت.

# جدول 3- 1برنامه های کاربردی مطالعه شده ( از بازار اندروید )



# 3-4 اعتبار سنجی بازیابی سورس کد

ما ازمایشات اعتبار سنجی گسترده ای از ded انجام دادیم. ازمایشات مشمول سورس کد های کوچک , متوسط و بزرگ برنامه های متن باز را بازیابی کرده و هیچ خطایی در بازیابی یافت نشد. در بیشتر موارد کد بازیابی شده واقعا از کد اصلی قابل تشخیص نبود.(کامنت های پیمانه ای و اسامی متغیر های محلی متد ها که شامل بایت کد نبود).

ما همچنین از ded برای بازیابی سورس کد ۵۰ برنامه کاربردی رایگان برتر (که در بازار اندروید فهرست شده بودند) از هر ۲۲ رده ی برنامه ها - ۱۱۰۰ تا در کل - استفاده کردیم. نسخه های برنامه هایی از بازار با استفاده از ابزار بازیابی عادی در ۱ سپتامبر ۲۰۱۰ بدست امدند. جدول یک امار دیکامپایل سازی ها را لیست کرده است. دیمامپایل کردن همه ی ۱۱۰۰ برنامه ۴۹۷.۷ ساعت (حدود ۲۰.۷ روز ) برای محاسبه زمان برد . سووت نشان داد که زمان پردازش ： ۹۹.۹۷ % زمان کل به زمان بهینه سازی و دیکامپایل کردن تعلق داشت. فرایند دیکامپایل قادر به بازیابی بیش از ۲۴۷ هزار کلاس گسترش یافته با ۲۱.۷ میلیون خط کد بوده است. این حدود ۹۴ % از کل کلاس هت در برنامه هاست. همه ی خطا های دیکامپایل کردن در طی دیکامپایل یا بعد از ان اشکار شد بنابرابن با مطالعه گزارش شده در قسمت های بعدی موافق بود. دو دسته خطا وجود دارد ：

خطا های بازگردانی ： ۰.۵۹% از کلاس ها بازگردانی نشدند. این خطا ها در سه کلاس اتفاق افتاد ：،الف . ارجاعات حل نشده که مانع بهینه سازی توسط سووت می شوند. ب. خطاهای نوع بوجود امده توسط کامپایلر dex اندروید و ج. موارد با نرخ بالایی که ded بایت کد غیر قانونی تولید کرده است. تلاش های اخیر بر بهبود بهینه سازی تمرکز داشته اند , مانند ded دوباره طراحی شده با یک ابزار استنتاج نوع تعریف شده ی صریح. کارهای هم راستا بر بهبود ded قادر به کاهش این خطاها به یک سوم بودند , و ما بهبود بیشتری در اینده نزدیک انتظار داریم.

خطاهای دیکامپایل کردن. ۵ % کلاس ها به طور کامل بازگردانی شده بود , اما سووت برای بازیابی سورس کد شکست خورد. در اینجا ما در وضعیت هنر دیکامپایل کردن محدود شدیم . به منظور درک مفهوم تاثیر دیکامپایل کردن کلاس های بازگردانی شده به فایل های معمولی class. جاوا توسط ded , ما یک مطالعه ی موازی برای ارزیابی سوت در برنامه های جاوا تولید شده با کامپایلر های سنتی جاوا انجام دادیم. از ۳۱۵۵۳ کلاس از یک تنوع از پکیج ها , سووت قادر به دیکامپایل کردن ۹۴.۵۹ % بود , نشان می دهد که ما نمی توانیم بهتر عمل کنیم تا وقتی که از سووت برای دیکامپایل کردن استفاده کنیم.

یک راه ممکن برای بهبود این استفاده از یک دیکامپایلر متفاوت است. پس از مطالعه ما فرن فلاور برای یک دوره کوتاه از یک ازمایش بتا امکان پذیر شده است . ما همین ۱۱۰۰ برنامه بهبود یافته را با استفاده از فرن فلاور دیکامپایل کردیم و یک نرخ بازیابی ۹۸.۰۴% از ۱.۶۵میلیون متد بازگردانی شده و- بهبود قابل توجه- داشتیم. مطالعات بعدی پایایی خروجی فرن فلاور و ورودی های نامناسب برای تجزیه و تحلیل برنامه را بررسی می کنند.

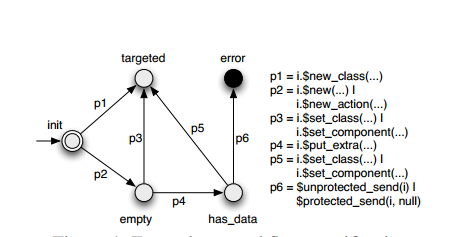
# 3-5 ارزیابی امنیت اندروید

مطالعه برنامه های اندروید ما شامل یک محدوده وسیع از ازمایشات متمرکز بر سه نوع تجزیه و تحلیل است ： الف. کاوش مسایل پوشش داده نشده در مطالعات قبلی و بحث بد افزار ها , ب. جستجو برای خطاهای امنیتی معمول کدنویسی , و ج. کاوش سو استفاده یا خطاهای امنیت در استفاده از چارچوب اندروید. در ادامه فرایند شناسایی و کد کردن ازمایشات بحث می شود.

# 3-6 ویژگی های تجزیه و تحلیل

ما ۴ روش ارزیابی سورس کد را استفاده کردیم ： تجزیه و تحلیل کنترل جریان , تجزیه و تحلیل کنترل داده , تجزیه و تحلیل ساختاری و تجزیه و تحلیل معنایی . مگر در موارد مشخص شده ی دیگر , همه ی ازمایشات از مجموعه ی تجزیه و تحلیل fortify SCA که این چهار نوع تجزیه و تحلیل را فراهم می کند , استفاده کردند . در ادامه برنامه های کاربردی رایج این روش ها بحث می شود. جزییات ویژگی های تجزیه و تحلیل ما می تواند در گزارش یافت شود.

تجزیه و تحلیل کنترل جریان. تجزیه و تحلیل کنترل جریان در دنباله ی اعمال اجراشده توسط یک برنامه ورودی P محدودیت هایی اعمال می کند و برخی از انها را به عنوان خطا طبقه بندی می کند. اساسا , یک قانون کنترل جریان یک اتوماتا A است که کلمات ورودی دنباله های اعمال P - مانند قانون نمایشات اجرای های P.- هستند. یک دنباله اعمال نادرست , ان است که A درون یک حالت خطای از پیش تعیین شده قرار می گیرد. برای به طور استاتیک اشکار کردن خطای مشخص شده ی A , برنامه هر مسیر کنترل جریان در مدل ابزار P را , به طور همگن , اجرای A در فعالیت های اجرا شده در طول این مسیر , پیمایش می کند. تا وقتی همه ی مسیر های کنترل جریان در مدل اجراهای P مرتب نشده اند , خطاهای مثبت امکان پذیر است. خطاهای منفی نیز در نظم , از طریق غیر معمول در عمل امکان پذیر است .شکل ۴ یک اتوماتا برای ارسال هدف را نشان می دهد. در اینجا حالت خطا پر شده است , اگر هدف شامل داده و محافظت نشده بدون مشخص شدن اجزای مقصد ارسال شود , در یک پتانسیل کمبود اطلاعات کاندید نشده حاصل می شود.



# شکل 3- 4مثال ویژگی های کنترل جریان

تجزیه و تحلیل جریان داده . تجزیه و تحلیل جریان داده مشحصات اعلانی مساله جریان های داده در برنامه ورودی را اجازه می دهد. برای مثال یک گوشی اندروید از چندید قطعه اطلاعات خصوصی نباید هیچ وقت تلفن را ترک کند , تشکیل شده است ： شماره تلفن کاربر , IMID (ایدی دستگاه) , IMSI ( ایدی مشترک ) و ICC-ID (شماره سریال سیم کارت) . در مطالعه ما , ما میخواهیم بررسی کنیم که این اطلاعات در شبکه نفوذ نکرده است. در حالیکه این ویژگی می تواند به طور منظم با استفاده از اتوماتا کد شود , مشخصات جریان داده امکان کدگذاری بسیار اسان تر را می دهد. مشخص کردن اعلانی برچسب های عبارات برنامه الگوهای نحوی برنامه را به صورت سورس های جریان داده و سینک ها تطبیق می دهد. جریان های داده بین سورس ها و سینک ها خطا محسوب می شود.

تجزیه و تحلیل ساختاری . تجزیه و تحلیل ساختاری امکان می دهد که الگوهای اعلان در نحو انتزاعی سورس کد ورودی تطبیق می خورد. مشخصات تجزیه و تحلیل ساختاری با اجراهای برنامه یا جریان داده ارتباط ندارد, بنابراین تجزیه و تحلیل محلی و سر راست است. به عنوان مثال در این مطالعه می خواهیم یک الگو تله جاییکه ی برنامه اندروید ایدی دستگاه ی تلفن در حال اجرا را استخراج می کند , مشخص کنیم. این الگو با استفاده از یک قانون ساختاری که که وقتی برنامه ورودی یک متد getDeviceIdکه درکلاس android.telephony.TelephonyManager جای دارد را فراخوانی می کند , حالت گرفته است , تعریف شده است.

تجزیه و تحلیل معنایی . تجزیه و تحلیل معنایی امکان مشخص کردن یک مجموعه محدود از محدودیت های مقادیر استفاده شده در برنامه ورودی را می دهد. برای مثال یک ویژگی مورد توجه مطالعه ما این است که یک برنامه اندروید پیام های اس ام اس را به مقصد های سخت کد شده نمی فرستد. برای بیان این ویژگی ما یک الگو با تطبیق فراخوانی های متد های پیام رسانی اندروید مانند sensTextMessage() تعریف کردیم. مشخصات معنایی به ما این اجازه را می دهد که مسقیما مشخص کنیم که پارامتر اول در این فراخوانی ها (شماره موبایل) یک ثابت نیست. تحلیلگر خطاهای این ویژگی را با استفاده از تکنیک های پخش ثابت که در ادبیات تحلیل برنامه به خوبی شناخته شده , اشکار می کند.

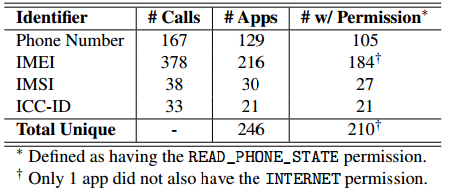
# 3-7 نتایج تحلیلی برنامه ها

در این قسمت نتایج تجزیه و تحلیل برنامه و بررسی دستی خطا های شناسایی شده را ثبت می کنیم.

سواستفاده اطلاعات

دراین قسمت ما کاوش می کنیم که چگونه اطلاعات حساس از طریق سینک های اطلاعات از جمله اشیا objectstream بازیابی شده از URLConnection , HTTP GET , پارامتر های POST در اتصالات httpclient ,و رشته استفاده شده برای اشیا url به بیرون درز می کند[۱۲،۱۴].کارهای آینده ممکن است همچنین شامل اس ام اس به شکل یک سینک باشد.

# جدول 3- 2دستیابی به شناسه هایAPI های تلفن



شناسه های تلفن

ما چهار شناسه ی تلفن را مطالعه کردیم:شماره تلفن،imei(شناسه ی دستگاه)،imsi(شناسه ی اشتراک)،و iccid(شماره سریال سیمکارت). ما دونوع تجزیه و تحلیل انجام دادیم:الف-ما apiها ک ب شناسه ها دستیابی دارند را اسکن کردیم و ما تجزیه و تحلیل جریان داده رابرای شناسایی قابلیت کد ارسال شناسه ها به شبکه استفاده کردیم.

جدول 2 خلاصه ی apiهای فراخوانی شده که شناسه های تلفن را دریافت میکنند نشام میدهد . در کل 246برنامه کاربردی (22.4%)مشمول کد برای بدشت آوردن یک شناسه تلفن بودند؛ با این حال فقط 210تا از این برنامه های کار بردی مجوز READ\_ PHONE\_STATEمورد نیاز برای دستیابی داشتند. قسمت 5.3کدی که برای مجوز پراب ها است را مورد بحث قرار میدهد.ما از جدول 2 که برنامه های کاربردی با دستیابی فراوان به imei(216برنامه کاردبردی ،19.6%) را مشاهده کردیم. شماره تلفن دومین بیشترین استفاده شده است( 129 برنامه کاربردی،11.7%) سرانجام imsiوiccidبسیار به ندرت استفاده شده اند( کمتر از3%) .

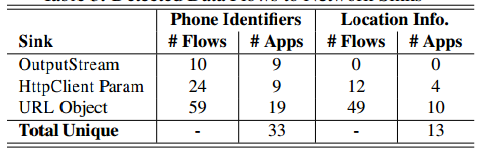
جدول 3 جریانهای داده که شناسه های تلفن را فیلتر میکنند نشان میدهد.33 برنامه کاربردی مجوزinternetدارند،اما یکدبرنامه کاربردی مجوز READ\_PHONE\_STATEنداشت.ما جریانهای داده ای برای همه ی 4نوع شناسه پیدا کردیم: 25 برنامه کاربردی جریان داده ی imeiدارند ؛10برنامه کاربردی جریان داده ی شماره تلفن دارند ؛ 5برنامه کاربردی جریان داده ی imsiدارند ؛ و چهار برنامه کاربردی جریان داده ی iccid دارند .

برای بدست آوردن یک درک بهتر از چگونگی استفاده ی شناسه های تلفن ، ما33 برنامه کاربردی شناسایی شده را بصورت دستی بررسی کردیم ، همچنین چندین برنامه کاربردی اضافه که شامل فراخوانی شناسه ی api ها هستند. ما فیلترهای همه ی برنامه های کاربردی بجز یکی را تایید کردیم. در این مورد پیچیدگی کد تایید دستی قبلی انجام شد؛ بهر حال ما یک جریان داده ی متفاوت یافت نشده بوسیله تجزیه و تحلیل برنامه را شناسایی کردیم تجزیه و تحلیل یافته های زیر را تشکیل میدهد .

یافته 1 - شناسه های تلفن پر تکرار از طریق درخاستهای متنی نفوذ کرده اند.اغلب سینکها پارامتر های httpget یا postهستند . نامهای پارامتر http برای imei عبارتند از “uid,” “user-id,” “imei,” “deviceId,” “deviceSerialNumber,” “devicePrint,” “X-DSN,”

and “uniquelycode”؛ نامهای شماره تلفن عبارتند از “phone” and “mdn”.؛ و نامهای imsi عبارتند از did” “ و "imsi.”. در یک مورد ما یک پارامتر http برای iccid شناسایی کردیم اما توسعه دهنده آنرا به اشتباه imei بچسب گذاری کرده بود.

# جدول 3- 3آشکارسازی جریان های داده برای سینک های شبکه



یافته 2- شناسه های تلفن ب عنوان دستگاه اثر انگشت استفاده شده اند . چندین جریان داده ما را به سمت کدی که فقط شناسه های تلفن را گذارش نکرده است هدایت کردند ، اما دیگر ویژگی های تلفن نیز برای یک سرور راه دور . برای مثال یک برنامه کاربردیه وال پیپر (com.eoeandroid.eWallpapers.cartoon) شامل یک کلاس با نام SyncDeviceInfosService که IMEI و صفت هایی مانند ورژن سیستم عامل و سخت افزار دستگاه را جمع آوری میکند ، هستند متود sendDeviceInfos() این اطلاعات را ب یک سرور میفرستد.

در برنامه کاربردی دیگری (com.avantar.wny) متود PhoneStats.toUrlFormatedString()یک رشته پارامتر URL شامل IMEI، مدل دستگاه ، پلت فرم ، و نام برنامه کاربردی ، ایجاد میکند . در حالی که هدف واضح نیست ، این اثر انگشت گیری نشان میدهد که شناسه های تلفن برای بیشتر از یک شناسه ی منحصر به فرد استفاده میشوند .

یافته 3 - شناسه های تلفن ، به خصوص IMEI برای حمله به کاربران فردی استفاده میشود . چندین برنامه کاربردی شامل کدی که IMEI را به عنوان یک شناسه منحصر به فرد به درخاستهای شبکه الحاق میکند ، هستند . برای مثال برخی برنامه های کاربردی ( مانند com.Qunar و

com.nextmobileweb.craigsphone) برای دسته بندی IMEI در جستوجوی پرس و جوها ظاهر شده اند؛ در ی برنامه کاربردیه مسافرتی (com.visualit.tubeLondonCity) متود (refreshLiveInfo) شامل هIMEI در یک URL است ؛ و یک برنامه کاربردی "حلقه کلیدی " (com.froogloid.kring.google.zxing.client.android) IMEI را به یک متغیر با نام retailerLookupCmd اضافه میکند . ما همچنین دریافتیم که قابلیتی که در IMEI وجود دارد هنگام برسی برای آپدیت ها ( مانند com.webascender.callerid .،که شامل شماره تلفن نیز هست ) و باز یابی تبلیغات ( یافته 6را ببینید ) است . علاوه بر این ما دو برنامه کاربردی (com.taobo.tao و raker.duobao.store) با .دستیابی متود های جدا کننده شبکه که شامل IMEI برای همه ی ارتباطات میباشد را پیدا کردیم این رفتارها نشان میدهد که IMEI به عنوان یک شکل از " حمله کوکی " استفاده میشود .

یافته 4- IMEI برای اطلاعات شناسه پذیر شخصی (PII) لازم است . اعتقاد رایج این است که IMEI برای نگاشت مالک تلفن خارج از شبکه سلولی قابل مشاهده نیست ک زیاد صحیح نیست. در چندین مورد ما کدی یافتیم که IMEI را به اطلاعات حساب و دیگر PII ها الحاق کرده است . برای مثال برنامه های (com.slacker.radio و com.statefarm.pocketagent) شامل IMEI در ثبت حساب و در خاست ورود است . در برنامه کاربردی دیگری (com.amazon.mp3) ، متود linkDevice() شامل IMEI است . بررسی کد نشان داد که این متود هنگامی که کاربر " ورود یک کد بالا برنده " را برای خرید کارتهای هدیه راانتخاب میکند ، فراخوانی شده است ما همچنین IMEI استفاده شده در کد برای ارسال کامنت ها و گذارش مشکلات پیدا کردیم ( مانند com.morbe.guarder و com.fm207.discount). سرانجام ما برنامه کاربردی یافتیم که (com.andoop.highscore)، دسته بندیIMEI هنگام ارسال بیشترین امتیازهای بازی آشکار میکند . بنا بر این این به وضوح دیده میشود که پایگاه داده های شامل نگاشت های بین کاربران فیزیکی و IMEI ها ایجاد میشود .

یافته 5- همه ی شناسه های تلفن برای اعمال فیلتر سازی را استفاده نکرده اند . چندین برنامه کاربردی که شناسه های تلفن دستیابی دارند مقادیر را فیلتر نکرده اند . برای مثال یک برنامه کاربردی (com.amazon.kindle) یک دستگاه اثر انگشت برای بررسی اعتبار سنجی ایجاد کرده است . اثر انگشت در " یک حافظه امن " نگه داری میشود و برای خروج از تلفن دیده نمیشود . برنامه کاربردی دیگری (com.match.android.matchmobile) شماره مبایل را به یک فیلد متنی مورد استفاده در ثبت نام حساب طراحی کرده است . در حالی که مقدار ارسال در طی ثبت نام به شبکه ارسال میشود ، کاربر میتواند به آسانی آنرا تغییر دهد یا حذف کند.

یافته 6- شناسه های تلفن به سرور های تحلیلی و تبلیغی ارسال میشوند بسیاری از برنامه ها تبلیغلت و قابلیتهای تحلیلی خاص دارند . برای مثال در یک برنامه کاربردی (com.accuweather.android) ، کلاس ACCUWXAdRequest یک سینک جریان داده IMEI است . برنامه کاربردی دیگری (com.amazon.mp3) جزو سرویس اندروید AndroidMetricsManagerتعریف کرده است که یک سینک جریان داده IMEI است . جریان های داده ی شناسه تلفن در کتابخانه های تبلیغی نیز رخ میدهند . برای مثال مایک سینک جریان داده ی شماره تلفن در کتابخانه ی com/wooboo/adlib\_android استفاده شده توسط چندین برنامه کاربردی ( مانند cn.ecook,

com.superdroid.sqd و com.superdroid.ewc) پیدا کردم . قسمت 5.3 کتابخانه های تبلیغی را با جزییات بیشتر مورد بحث قرار میدهد .

اطلاعات محل

اطلاعات محل به دو شیوه عرض یابی شد:1 فراخوانی getLastKnownLocation، و تعریف بازخورد در یک شی LocationListener ارسال شده به requestLocationUpdates به دلیل خطاهای بازیابی کد همه ی شی های LocationListener، فراخوانی requestLocationUpdates متناظر را ندارند . ما همه 3 سازنده را عرض یابی میکنیم .

جدول 4 دستیابی های محل اطلاعات را خلاصه کرده است ، 505 برنامه کاربردی ( 45.9%) برای دستیابی به محل تلاش کرده اند ، فقط 304 تا ( 27.6%) مجوز انجام آنرا داشتند. این تفاوت مشابه آن در کتابخانه هایی که برای مجوزها پراب شده اند است . فاصله ی بین LocationListener و requestLocationUpdates() به شکل مقدماتی برای کتابخانه AdMob است ، که شکل دهنده تعریف شده است اما بدون فراخوانی های بعد .

جدول 3 جریانهای داده ی محل برای شبکه را نشان میدهد برای باز گردانی چالش های کد های گم شده ، سرس جریان داده به شکل متد های getLatitude() و getLongitude() از شی Location باز یابی شده از API های موقعیت تعریف شده است. ما 13 برنامه کاربردی با جریانهای داده محل را به صورت دستی بررسی کردیم. بسیاری از جریانهای داده برای بازتاب کاربردهای قانونی از محل هر یک از طبقه بندی ها ، نقاط مورد علاقه و سرویس های شبکه های اجتماعی آماده شده اند . بررسی برنامه های کاربردی باقی مانده به شکل یافته های زیر است :

یافته 7- قطعه قطعه کردن محل گزارش محل ممکن نیست همیشه با یک کاربر دیده شود . در یک برنامه (com.andoop.highscore) هر دوی شهر یا کشور و مختصات جغرافیایی همراه با امتیازهای بالا ارسال میشدند. کاربران ممکن است از اطلاعات جغرافیایی محلی مرتبط با امتیازها آگاه باشند ، اما این واضح نیست که اکر کاربران آگاه باشند که مختصات دقیق نیز استفاده شده باشد .

یافته ی 8- اطلاعات محل به سرور های تبلیغاتی ارسال میشوند چندین جریان داده محل آشکار شده برای پایان در اتصلات شبکه برای بازیابی آگهی ها استفاده شده است. برای مثال دو برنامه کاربردی (com.avantar.wny و com.avantar.yp ) محل را به متغیر webAdURLString اضافه کرده اند با بررسی [14]،ما کتابخانه Admob را برای تعیین این که چرا هیچ جریان داده ای یافت و تعیین نشد و که خطاهای بازیابی سرس کد منجر به خطاهای منفی میشود ، بررسی کردیم .

سو استفاده تلفن

این قسمت سواستفاده های رابط های گوشی های هوشمند ، شامل سرویس های تلفن ، ضبط صدا و تصویر پس زمینه ، سوکتها ، و دستیابی به لیست برنامه های نصب شده را کاوش میکند.

سرویس های تلفن

بد افزار های گوشی های هوشمند میتوانند دسیابی مستقیم فراهم کنند با استفاده از تماسهای تلفن یا پیام های اس ام اس برای شماره های پولی ما سه پرس و جو برای شناسایی رفتار این مخربها تعریف کرده ایم: 1 ثابت استفاده شده برای شماره های مقصد اس ام اس ؛ 2 ایجاد اشای URI با یک پیشوند " TEL:" ( استفاده شده برای هدف پیامهای تماس تلفنی ) و رشته ی " 900 " ( یک پیشوند شماره پولی در امریکا) ؛ و 3 هر شی UIR با یک پیشوند TEL. تحزیه و تحلیل یافته های زیر را تشکیل میدهد .

یافته 9- برنامه های کاربردی برای استفاده از سرویسهای شماره تلفن ثابت آماده نمیشوند . ما صفر برنامه کاربردی که از یک ثابت شماره مقصد برای API اس ام اس استفاده میکنند ، یافتیم توجه کنید که ویژگیهای تجزیه و تحلیل ما با ثابتهای ارسال شده به طور مستقیم API و متغیر های FINANL محدود شده است و بنا بر این ممکن است خطاهای منفی داشته باشد . ما دو برنامه کاربردی یافتیم که اشیا URI با پیشوند " TEL: " و شامل رشتهی "900" تیجاد میکنند . یک برنامه کاربردی شامل کد برای فراخوانی <tel://0900-9292> ، که یک شماره پولی (70 سنت در دقیقه)است که برای مشاوره سفر در نترلند است . با این حال این یک تخریب محسوب نمیشود ، به مانند برنامه کاربردی (com.Planner9292) طراحی شده برای فراهم کردن مشاوره سفر . برنامه کاربردی دیگری از چندین شماره ی سخت کدشده با "900" در چهار رقم آخر شماره است .نتایج تجزیه و تحلیل پولی و اس ام اس شاخص ها را نسبت به عدم وجود رفتار مخرب اطمینان میدهد . تجزیه و تحلیل های آینده باید پیشوندهای پولی بیشتری را شامل شود .

یافته 10- برنامه های کاربردی برای سواستفاده سرویس های صوتی آماده نمیکنند . ما 468 شی URI با پیشوند "TEL:" در 358 برنامه کاربردی یافتیم . ما یک نمونه از برنامه های کاربردی برای درک بهتر استفاده شماره تلفن به صورت دستی بررسی کردیم . ما دریافتیم که 1 برنامه های کاربردی پر تکرار شامل قابلیت فراخوانی سرویسهای مشتری هستند ؛ 2 فعالیتهای هدف “CALL”و“DIAL” به طور یکسان برای هدف یکسان استقاده شده بودند (CALL بلافاصله فراخوانی شده و نیاز به مجوز CALL\_PHONE دارد ، در حالی که DIAL تایید گیرنده کاربر دارد و به هیچ مجوزی نیاز ندارد ) ؛ و 3 همه ی شماره های تلفن سخت کد شده برای ایجاد تماسهای تلفن استفاده شده اند ، مانند کتابخانه AdMob ظاهرا یک شماره تلفن سخت کد شده ی بلااستفاده داشت .

صدا و تصویر پس زمینه

استراق صمع دوربین و میکروفن در گوشی های هوشمند یک نگرانی واقعی است [41] . ما رفتار استراق صمع برنامه ی ماربردی را تجزیه و تحلیل کردیم ، بویژه: 1 ضبط تصویر بدون فراخوانیsetPreviewDisplay() (این API همیشه برای ضیط تصویر مورد نیاز است) ؛ 2 ... در کد از یک جزو فعالیت اندروید قابل دسترس نیست ؛ و 3 AudioRecord.read در کد از یک جزو فعالیت قابل دسترس نیس .

یافته 11- برنامه های کاربردی برای سواستفاده ی ضبت ویدیو آماده نیستند. ما هیچ برنامه کاربردی که تصویر را بدون فراخوانی setPreviewDisplay ضبط کند نیافتیم . جست و جو قطعا شامل مقادیر ارسال شده به نمایش صفحه نمایش نیست ، و بنابراین ممکن است خطاهای منفی ایجاد شود . برای مثال [ نمایش صفحه نمایش] شاید در اندازه یک پیکزل باشد . پرس و جوی MediaRecorder.start ضبط صدا را آشکار میکند ، اما ضبط تصویر را نیز آشکار میکند . این پرس و جو دو برنامه کاربردی با استفاده از تصویر در کد از یک فعالیت قابل دسترسی نیست را یافت؛ با این حال کلاس های SurfaceView ، اضافه شده بود که به وسیله setPreviewDisplay. استفاده میشد .

یافته 12 - برنامه های کاربردی برای سواستفاده ضبط صدا آماده نیستند . ما هشت کاربرد در هفت برنامه کاربردی از AudioRecord.read بدون یک مسیر کنترل جریان یک جزو فعالیت یافتیم . از این برنامه های کاربردی سه قابلیتVOIP موجود است ، دوتا بازی که چیزی که کاربر میگوید را تکرار میکنند ، و یک جست و جوی صوتی فراهم میکنند. در این برنامه های کاربردی ضبط صدا انتظار میرود ؛ کمبود توانایی دسترسی مشابه آن در شکست های باز یابی کد وجود دارد برنامه های کاربردی باقیمانده مجوز RECORD\_AUDIO مورد نیاز ندارنند و باید مانند بخشی از یک جعبه ابزار کد نویسی شوند. پرس و جوی ... 5 برنامه کاربری اضافیه ضیط صوت بدون قابلیت دسترسی به یک فعالیت را شناسایی کرد . سه تا از این برنامه ها دلیل قانونی برای ضبط صدا دارند: جست و جوی صوتی ، بازی محاوره ای و VOIP . سر انجام دو بازی شامل ضبط صدا در یک جعبه ابزار توسعه دهنده بودند ، اما بدون هیچ مجوز ضبط ، که کمبود قابلیت دسترسی را توضیح میدهد . قسمت 5.3.2 در مورد جعبه ابزار توسعه دهنده بحث میکند.

استفاده ی API سوکت

سوکتهای جاوا یک رابط باز برای سرویسهای خارجی ارایه میدهد ، و بنابر این یک منبع بالقوه از رفتار مخرب است. برای مثال بات نت های بر پایه ی گوشی های هوشمند برای وجود بر آیفون های “jailbroken” یافت شد [8] . ما نشان دادیم که اغلب برنامه های کاربردی اینترنت محور گوشی های هوشمند کلاینتهای Http هستند . اندروید شامل کلاسهای مفیدی است( مانند HttpURLConnection و HttpClient ) برای ارتباط با سرور های وب .بنا براین ما برای برنامه های کاربردی که ارتباط شبکه با استفاده از کلاس سوکت ایجاد میکنند پرس و جو میکنیم .

یافته 13 - یک تعداد کوچک از برنامه های کاربردی شامل کدی هستند که از کلاس سوکت مستقیما استفاده میکند . ما 177 ارتباط سوکت در 75 برنامه کاربردی ( 6.8%) یافتیم. بسیاری از برنامه های کاربردی برای داشتن کتابخانه های شبکه ی به خوبی شناخته شده مانند org/apache/thrift, org/apache/commons و org/eclipse/jetty ، که از سوکت ها مستقیما استفاده میکنند علامت خورده اند سازنده های سوکت نیز تشخیص داده شدند . نامهای سازنده های شناسایی شده مانند AllTrustSSLSocketFactory و NonValidatingSSLSocketFactory به عنوان پتانسیل آسیب پذیری مورد توجه اند ، اما ما هیچ شواهدی از استفاده مخرب نیافتیم . چندین برنامه کاربردی نیز شامل متود های جدا کننده ی HTTP خود که قابلیت تکرار در کتابخانه های اندروید را دارند ، هستند ، اما مخرب ظاهر نشدند . در میان برنامه های کاربردی شامل جدا کننده های ارتباط شبکه ی سفارشی یک گروه از برنامه ها در رده ی [ مالی ] پروتوکل های شبکه ی نهفته را تکرار میکنند ( مانند ، در com/lumensoft/kslibrary ) . ما توجه داشتیم که این برنامه های کلربردی از مجموعه کاراکتر های آسیایی برای توصیف بازارشان استفاده میکنند و ما نتوانستیم هدف دقیق آنها را تعیین کنیم .

یافته14 - ما در یافتیم ک هیچ شواهدی از رفتار مخرب توسط برنامه هایی که از سوکت به شکل مستقیم استفاده میکنند وجود ندارد. ما به صورت دستی همه 75 برنامه معین شده را بررسی کردیم اگر سوکت از ابزار مناسب بر مبنای توصیف برنامه استفاده کند . بررسی ما یک آرایه ی معکوس از کاربرد های سوکت را بدست آورد شامل: پروتوکل های انتقال فایل ، پروتوکولهای چت ، جریانهای ویدیو و صدا ، و اتصال شبکه ها به هم ، در میان کاربردهای دیگر از خلاصه حذف شدند. یک برنامه ی کامل اتصالات سوکت برای ای پی آدرس و پورت خای غیر استاندارد سخت کد شده دارد .برای مثال یک برنامه کاربردی (...) کمک ها را از 208.94.242.218 بر روی پورت 2009 دانلود میکند. علاوه بر این دو برنامه کاربردی مالی بررسی نشده (com.miraeasset.mstock و kvp.jjy.MispAndroid320) شامل کتابخانه kr/co/shiftworks که به 209.85.227.147 بر روی پورت 9001 متصل میشود ، است . علاوه بر این یک برنامه کاربردی (com.tf1.lci) به 209.85.227.147 بر روی پورت 80 در یک کلاس بل نام AdService و فراخوانی های بعدیه getLocalAddress() برای بازیابی IPآدرسهای تلفن متصل میشود . در کل ما در یافتیم که هیچ نوع شواهدی از رفتار مخرب وجود ندارد ، اما چندین برنامه کاربردی بررسی های عمیق تر طلب میکنند .

# 3-8 برنامه های کاربردی نصب شده

برنامه های کاربردی نصب شده داده های بازار یابی با ارزشی فراهم میکنند . اندروید دو نوع ای پی آی مرتبط دارد:

1 . یک مجموعه از ای پی آی های گت لیست برنامه های نصب شده یا اسامی بسته ها را باز میگرداند ؛ و 2. یک مجموعه از ای پی آی های پرس و جو که وضوح هدف زمان اجرای اندروید را منعکس میکنند ، اما میتوانند ژنریک ساخته شوند .

یافته 15 - برنامه های کاربردی نمیتوانند اطلاعات کاربردی مخرب درباره ی این برنامه های کاربردی نصب شده بر روی تلفن محیا کنند . در همه بجز دو مورد ، برنامه های کاربردی نمونه سازی شده با استفاده از ای پی آی های GET نتایج یک برنامه ی کاربردی خاص را جست و جو میکنند. یک برنامه کاربردی (com.davidgoemans.simpleClockWidget) یک متود که لیست همه برنامه های کاربردی نصب شده را باز میگرداند ، تعریف کرده است ، اما نتایج فقط به کار بر نمایش داده میشود . برنامه کاربردی دوم (raker.duobao.store) یک متود مشابه تعریف کرده است ، اما فقط برای فراخوانی شدن توسط کدهای ترجمه شده ی بلااستفاده فراهم میشود .

یافته 16 – کتابخانه آگهی و تجزیه و تحلیل که استفاده می کند از شناسه های تلفن و محل گاهی اوقات قابل پیکربندی است. کتابخانه تجزیه و تحلیل com/webtrends/mobile (استفاده شده توسط com.statefarm.pocketagent)، کلاس WebtrendsIdMethod را تعریف می کند که چهار نوع شناسه را مشخص می کند. فقط یک نوع، "سیستم شناسه گسترش" از شناسه های تلفن (IMEI، IMSI و ICC-ID) استفاده می کند. معلوم نیست که چه نوع شناسه توسط نرم افزار مورد استفاده قرار گرفت. کتابخانه های دیگری پیکربندی مشابه فراهم می کنند. به عنوان مثال، مستندات ادموب در SDK [6] نشان می دهد که فقط شامل اطلاعات محل است اگر پیکربندی آشکار بسته ان را فراهم کند.

یافته 17 - تجزیه و تحلیل فرکانس گزارش کتابخانه اغلب قابل تنظیم است. در طول بررسی دستی، ما با یک نرم افزار (com.handmark.mpp.news.reuters) مواجه شدیم که در آن شماره تلفن به FlurryAgent.onEvent() به عنوان داده کلی منتقل می شود. این متد در سراسر برنامه فراخوانی می شود، و برچسب های رویداد را مانند “GetMoreStories” ، “StoryClickedFromList” و “ImageZoom” مشخص می کند. در اینجا، کد برنامه اصلی را مشاهده می کنیم که نه تنها شماره تلفن را برای گزارش مشخص می کند، بلکه فرکانس را نیز گزارش می دهد.

یافته 18 – کتابخانه آگهی و تجزیه وتحلیل برای مجوز کاوش می کند. کتابخانه com/webtrends/mobile به IMEI، IMSI، ICC-ID و محل دسترسی پیدا می کند. کلاس (WebtrendsAndroidValueFetcher) از بلوک های try/catch استفاده می کند که از SecurityException بدست می آید و هنگامی که یک برنامه مجوز لازم را ندارد پرتاب می شود. قابلیت مشابه در کتابخانه com/casee/adsdk وجود دارد (استفاده شده توسط com.fish.luny). در AdFetcher.getDeviceId، متد checkCallingOrSelfPermission اندروید قبل از دسترسی به IMSI مورد بررسی قرار می گیرد.

یافته 19 - برخی از بسته های ابزار توسعه دهنده قابلیت های خطرناکن را بر می گردانند. ما سه برنامه کاغذ دیواری توسط توسعه دهنده "callmejack" یافتیم که شامل خدمات در مسیر کتابخانه com/jackeeywu/apps/eWallpaper هستند (com.eoeandroid.eWallpapers.cartoon، com.jackeey.wallpapers.all1.orange و com.jackeey. eWallpapers.gundam). این کتابخانه دارای سینک های جریان داده برای شماره تلفن، IMEI، IMSI و ICC-ID است. در ماه ژوئیه سال 2010، شرکت Lookout، یک برنامه کاغذ دیواری توسط توسعه دهنده “jackeey,wallpaper” گزارش داد بطوریکه این شناسه ها را به imnet.us ارسال می کرد [29]. این گزارش همچنین نشان داد که توسعه دهنده نام خود را به "callmejack" تغییر داد. در حالی که برنامه اصلی “jackeey,wallpaper” از بازار اندروید حذف شده بود، برنامه کاربردی توسط "callmejack" از تاریخ سپتامبر 2010.3 باقی ماند.

یافته 20 – برخی از جعبه ابزار توسعه دهندگان برای مجوزها کاوش می کنند. در یک برنامه (com.july.cbssports.activity)، کدی در کتابخانه com/julysystems است که متد checkPermission() اندروید را برای مجوزهای READ\_PHONE\_STATE و ACCESS\_FINE\_LOCATION قبل از دسترسی به شماره IMEI، شماره تلفن، و آخرین موقعیت مکانی شناخته شده، به ترتیب ارزیابی می کند.

برنامه دوم (v00032.com.wordplayer) کلاس CustomExceptionHander برای ارسال یک رویداد استثنا به URL HTTP تعریف می کند. کلاس برای بازیابی شماره تلفن در داخل یک بلوک try / catch، ابتلا به استثنا عمومی تلاش می کند. با این حال، برنامه مجوز READ\_PHONE\_STATE را ندارد، نشان می دهد کلاس به احتمال زیاد در برنامه های متعدد استفاده می شود.

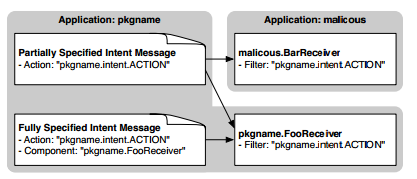
یافته 21 – مارک های شناخته شده گاهی اوقات ماموریت می دهند به توسعه دهندگانی که شامل قابلیت های خطرناک هستند. جعبه ابزار توسعه دهندگان com/julysystems که به عنوان کاوش برای مجوزها تعریف شده در دو برنامه با ارائه دهندگان نرم افزار معتبر وجود دارد. "شبکه CBS ورزشی طرفدار فوتبال" (com.july.cbssports.activity) که توسط "شرکت تعاملی سی بی اس" ارائه شده، و "به اشتراک گذاری فوتبال" (com.july.univision) که توسط "شرکت اشتراک گذاری رسانه های تعاملی" ارائه شده است. هر دو دارای مجوز مکان و وضعیت گوشی هستند، و از این رو به طور بالقوه از اطلاعات سوء استفاده می کنند.

به طور مشابه، "ایالات متحده آمریکا امروز" (com.usatoday.android.news) ارائه شده توسط "ایالات متحده آمریکا امروز" و "فاکس نیوز" (com.foxnews.android) ارائه شده توسط " شبکه خبر فاکس،اطلاعات LLC" شامل جعبه ابزار com/mercuryintermedia می باشند. هر دو برنامه شامل یک مؤلفه فعالیت آندروید به نام MainActivity هستند. در مرحله اولیه، IMEI بازیابی می شود و به ProductConfiguration.initialize() می رسد (بخشی از جعبه ابزار com/ mecuryintermedia). هر دو برنامه دارای شماره IMEI برای شبکه جریان داده از طریق این روش هستند.

یافته 22 - اطلاعات خصوصی در رابط ورود به سیستم عمومی آندروید نوشته شده است. ما 253 جریان داده در 96 برنامه برای اطلاعات محل، و 123 جریان در 90 برنامه برای شناسه تلفن یافتیم. غالبا، URL های حاوی این اطلاعات خصوصی درست قبل از یک اتصال به شبکه ساخته شده، وارد شده است. بنابراین، مجوز READ\_LOGS اجازه دسترسی به اطلاعات خصوصی می دهد.

نشت اطلاعات از طریق IPC

در شکل 5 نشان داده شده، هر برنامه می تواند انتشارات قطعی دریافت کند که مولفه هدف را مشخص نمی کند و یا از پخش با مجوز حمایت نمی کند (نوع مجوز نشان داده نشده است). این نا امن است اگر هدف حاوی اطلاعات حساس باشد. 271 انتشار قطعی اینچنین نا امن را با داده “extras” در 92 برنامه (٪ 8.4) یافتیم. نمونه این برنامه ها، ما چندین مفاهیم مورد استفاده برای نصب کلیدهای میانبر به صفحه اصلی یافتیم.



# شکل 3- 5استراق سمع در مفاهیم محافظت نشده

یافته 23 – برنامه هایی اطلاعات خصوصی در IPC را به تمام برنامه های کاربردی قابل دسترس منتشر کردند. ما نمونه های بسیاری از برنامه های ارسال مفاهیم نا امن برای اقدام رشته ها شامل فضای نام برنامه (به عنوان مثال، "pkgname.intent.ACTION" برای درخواست pkgname) یافتیم. محتویات اطلاعات همراه متفاوت بود. در برخی موارد، داده ها حساس نبودند، به عنوان مثال، ویجت و شناسه کار. با این حال، ما نیز اطلاعات حساس را یافتیم. به عنوان مثال یک نرم افزار (com.ulocate) مکان کاربر را به "com.ulocate.service.LOCATION" رشته فعالیت هدف بدون محافظت، منتشر می کند. در برنامه دیگری (com.himsn) وضعیت پیام های فوری مشتری را به رشته فعالیت "cm.mz.stS" منتشر می کند. این آسیب پذیری به برنامه های مخرب اجازه استراق سمع از اطلاعات حساس در IPC را می دهد، و در برخی موارد، دسترسی به اطلاعاتی که نیاز به مجوز دارند را فراهم می کند (به عنوان مثال، محل).

گیرنده های پخش حفاظت نشده

برنامه های کاربردی از اجزای گیرنده پخش برای دریافت پیام مقصد استفاده می کند. گیرنده های پخش "فیلتر مقصد" برای عضویت در انواع رویداد خاص که عمومی اند، تعریف می کند. اگر گیرنده توسط یک مجوز محافظت نشود، برنامه مخرب می تواند پیام را جعل کند.

یافته 24 – تعداد معدودی از برنامه های آسیب پذیر حملات به گیرنده های پخش پویا را جعل می کنند. 406 گیرنده پخش محافظت نشده در 154 برنامه کاربردی (14٪) یافتیم. تعداد زیادی از گیرنده های مشترک با انواع سیستم تعریف شده مقصد یافتیم. این گیرنده ها به صورت غیر مستقیم توسط "پخش برنامه های مصون" آندروید معرفی شده برای از بین بردن جعل محافظت می شوند. نرم افزاری با گیرنده پخش بدون محافظت برای یک نوع مقصد سفارشی یافتیم. با این حال به نظر می رسد دارای تاثیر محدود است. نمونه برداری اضافی کشف موارد بیشتر را ممکن می سازد.

# 3-9 حملات تزریقی مقصد

پیام های مقصد نیز برای شروع فعالیت و خدمات قطعات استفاده می شود. اگر آدرس مقصد از ورودی نامطمئن به دست آمده، یک حمله تزریقی مقصد رخ می دهد. 10 جریان داده از شبکه به یک آدرس مقصد در 1 برنامه کشف کردیم. ما نمی توانستیم جریان داده را تایید و آن را مثبت کاذب طبقه بندی کنیم. سینک جریان داده ها در یک کلاس به نام ProgressBroadcastingFileInputStream وجود دارد. ارجاعات بدون کد دیکامپایل شده این کلاس، و همه منابع جریان داده به URLConnection.getInputStream() فراخوانی می شود، که برای ایجاد اشیاء InputStreamReader استفاده شده است. ما معتقدیم خطاهای مثبت از آنالیز برنامه مدل سازی کلاس های توسعه دهنده InputStream حاصل می شود.

80 جریان داده از IPC به یک آدرس مقصد در 37 برنامه کاربردی می یابیم. جریان داده را با استفاده از سینک طبقه بندی کرد: تابع سازنده مقصد سینکی برای 13 برنامه کاربردی است؛ setAction سینکی برای 16 برنامه؛ و setComponent سینکی برای 8 برنامه است. این مجموعه متلاشی شده است. از 37 برنامه های کاربردی، ما متوجه شدیم که 17 برنامه صراحتا اجزای کلاس هدف را قرار داده است (همه بجز 3تا از سینک جریان داده setAction() استفاده می کنند)، به عنوان مثال، تقویت کردن رشته فعالیت از یک گیرنده پخش به یک سرویس. همچنین چهار خطای مثبت یافتیم به سبب فرض ما که همه اشیاء مقصد از IPC می آید (چند مورد استثنا وجود دارد). برای 16 مورد باقیمانده، مشاهده می کنیم:

یافته 25 - بعضی از برنامه ها آدرس مقصد را بر اساس ورودی IPC تعریف می کنند. سه برنامه از رشته ورودی IPC برای تعیین بسته بندی و نام اجزا برای سینک جریان داده setComponent استفاده می کنند. به طور مشابه، یک نرم افزار ورودی "اضافی" IPC را برای تعیین اقدام تابع سازنده مقصد استفاده می کند. بر اساس رشته فعالیت بازگشتی در نتیجه فعالیت های شروع شده قبلی، دو برنامه فرعی فعالیتی را آغاز می کنند. با این حال، با استخراج این آسیب پذیری، برنامه ها ابتدا باید فعالیت مخرب را شروع کنند. در موارد باقی مانده، رشته فعالیت مورد استفاده برای شروع یک جزء به طور مستقیم به یک شی جدید مقصد کپی شده است. یک برنامه مخرب می تواند از این آسیب پذیری با مشخص کردن نام جزء آسیب پذیر به طور مستقیم و کنترل رشته فعالیت بهره برداری کند.

کنترل واگذاری

برنامه ها می توانند با استفاده از یک "در انتظار مقصد" فعالیت را به یک برنامه دیگر محول کنند. برنامه ابتدا یک پیام مقصد ایجاد می کند که عمل انجام شده است. سپس یک ارجاع به مقصد بر اساس نوع مولفه هدف ایجاد می کند (محدود کردن چگونگی توانایی استفاده ان). گیرنده مقصد معلق نمی تواند مقادیر را تغییر دهد، اما می تواند فیلدهای گم شده را پر کند. بنابراین، اگر آدرس مقصد نامشخص باشد، نرم افزار کنترل از راه دور می تواند هدایت کند عملی که با مجوزهای برنامه اصلی انجام شده است.

یافته 26 – تعداد معدودی از برنامه ها بطور نا امن اقدامات را نمایندگی می کنند. 300 اشیاء در انتظار مقصد ناامن در 116 برنامه کاربردی (10.5٪) یافتیم. در نمونه برداری از این برنامه ها، ما تعداد قریب به اتفاق مفاهیم در انتظار استفاده برای هر کدام را دریافتیم: (1) خدمات اطلاع رسانی UI آندروید؛ (2) خدمات زنگ آندروید؛ و یا (3) برقراری ارتباط بین یک ویجت UI و برنامه اصلی. هیچ یک از این موارد اجازه دستکاری توسط یک برنامه مخرب نمی دهند. دو برنامه کاربردی یافتیم که در انتظار ارسال مفاهیم نا امن از طریق IPC می باشد. با این حال، به نظر می رسد بهره برداری از این آسیب پذیری استفاده خصمانه ناچیز را فراهم می کند. همچنین توجه داشتیم که بیشتر از یک چارچوب تجزیه و تحلیل پیچیده تر برای از بین بردن خطای مثبت فوق می تواند مورد استفاده قرار گیرد.

# 3-10 کار مرتبط با امنیت

ابزارها و تکنیک های بسیاری برای شناسایی نگرانی های امنیتی در نرم افزار طراحی شده اند. نرم افزار نوشته شده در C به خصوص به اشتباهات برنامه نویسی که منجر به آسیب پذیری می شود، حساس است. اشکرفت و انگلر [7] برای شناسایی خطاهای موجود در محدوده بررسی ها الحاقات کامپایلر را استفاده می کنند. MPOS از بررسی مدل نسبت به مقیاس مقدار زیادی از کد منبع استفاده می کند. برنامه های جاوا ذاتا امن تر از برنامه های C هستند و از آسیب پذیری های ساده مانند سرریزهای بافر اجتناب می کنند. شبکه و فاکس هشت منبع مختلف باز و ابزار تجزیه و تحلیل کد منبع جاوا تجاری در دسترس را مقایسه می کنند، و پی می برند ابزاری که تمام آسیب پذیری را تشخیص دهد، وجود ندارد. Hovemeyer و پاف شش برنامه محبوب جاوا و کتابخانه های استفاده کننده FindBugs گسترش یافته با چک های اضافی را مطالعه کردند. در حالی که تجزیه و تحلیل شامل اشکالات غیر امنیتی، نتایج ایجاد انگیزه یک نیاز قوی برای تجزیه و تحلیل خودکار تمام توسعه دهندگان است. Livshits و لام بر روی برنامه های وب مبتنی بر جاوا تمرکز می کنند. در محیط سرور وب، ورودی به راحتی توسط دشمن کنترل می شود، ودر چپ بدون کنترل می تواند به تزریق SQL ، اسکریپت نویسی بین سایتی، HTTP جداکننده پاسخ، مسیر پیمایش، و تزریق دستور منجر شود. Felmetsger و همکاران نیز برنامه های وب مبتنی بر جاوا را مطالعه کردند. آنها تجزیه و تحلیل آسیب پذیری را با فراهم آوردن تشخیص خودکار خطاهای منطقی برنامه خاص بهبود دادند.

نرم افزارهای نقض کننده جاسوسی و حفظ حریم خصوصی نیز مورد مطالعه قرار گرفته است. Kirda و همکاران خواص رفتاری BHOs و نوار ابزار را می سنجند. Egele و همکاران نشتی اطلاعات توسط نرم افزارهای جاسوسی مبتنی بر مرورگر را صریحا با استفاده از تجزیه و تحلیل عیب پویا هدف قرار دادند. Panaorama نرم افزارهای مخرب نقض کننده حریم خصوصی را به طور کلی با استفاده از کل سیستم، و ردیابی عیب های کوچک می سنجد. حفظ حریم خصوصی اوراکل از دیفرانسیل جعبه سیاه آزمون ریش ریش شدن برای پیدا کردن نشت حریم خصوصی در برنامه های کاربردی استفاده می کند.

در گوشی های هوشمند، TaintDroid از سیستم گسترده ردیابی عیب پویا برای شناسایی نشتی حریم خصوصی در برنامه های کاربردی آندروید استفاده می کند. با استفاده از تجزیه و تحلیل ایستا، ما قادر به مطالعه تعداد بسیار بیشتری از برنامه های کاربردی (1100 در مقابل 30) بودیم. با این حال، تجزیه و تحلیل TaintDroid خروج از اطلاعات تایید می کند، در حالی که تجزیه و تحلیل ایستای ما تنها پتانسیل برای ایجاد آن را تایید می کند. گیرین همچنین از تجزیه و تحلیل پویا استفاده می کند، اما بر مجوز و سایر داده های پیکربندی برنامه نیز تمرکز دارد، در حالی که مطالعه ما بر تجزیه و تحلیل کد منبع. در نهایت، PiOS آنالیز ایستا در برنامه های کاربردی iOS برای آی فون انجام می دهد. مطالعه PiOS اکثر برنامه های کاربردی تجزیه و تحلیل برای نشت ID دستگاه و بیش از نیمی از برنامه های کاربردی شامل تبلیغات و تجزیه و تحلیل کتابخانه را پایه ریزی کرد.

# 3-11 مرور برنامه ی امنیتی اندروید

در اوایل توسعه تیم توسعه هسته اندروید شروع به بازشناختی کردن تا مدل امنیتی پر قدرت که نیاز فعال کردن اکوسیستم نیرومند برنامه ها و دستگاها پلتفرم اندروید است فراهم شود و از سرویس های ابری نیز پشتیبانی شود.

مولفه های کلیدی برنامه های امنیتی اندروید به شرح زیر است :

# 3-12 بازنگری طراحی

فرایند امنیتی اندروید اوایل، اوایل چرخه توسعه با شناختن طرح و مدل امنیتی کامل و پیکربندی پذیر شروع شد. هر خصوصیت مهم پلتفرم و منابع امنیتی و مهندسی بازنگری شد و با کنترلهای امنیتی بهتر با معماری ساختاری سیستم یکی شد.

# 3-13 تست نفوذپذیری و بازنگری کدها

در طول توسعه پلتفرم اجزا (Components) متن باز و برای اندروید ساخته شده در بازنگری شدید امنیتی قرار گرفتن. این بازنگری توسط تیم امنیتی اندروید یعنی تیم مهندسی امنیت اطلاعات گوگل و مشاوران امنیتی مستقل صورت گرفت. هدف از این فعالیت ها شناخت ضعف ها و آسیب پذیری های بلقوه قبل از انتشار بود.

# 3-14 بازنگری Opensource و انجمنها

پروژه ی اندروید مشتاق است که هر متخصص و علاقه مند به توسعه آن کمک کند. و در مورد انجمن، مکانهایی همچون گوگل پلی امکان ارتباط مستقیم با مردم را نیز میدهد.

# 3-15 واکنش به مشکلات

بصورت تمام وقت تیم امنیتی اندروید، تمام موضوعات امنیتی مطرح شده در انجمنها را در هر لحظه رصد میکنند تا با تمام آسیب پذیری های احتمالی واقف باشند و آنها را سریعا مرتفع کنند. و درنهایت خطر استفاده از اندروید را برای کابران به حداقل برسانند.

# 3-16 معماری امنیتی پلتفرم اندروید

اندروید به دنبال این است که به امنترین و پرکاربردترین سیستم عامل برای پلتفرمهای موبایل تبدیل بشود.اندروید کنترلهای امنیتی سیستم عامل های معمولی را که شامل موارد زیر است را دارد :

* حفاظت از اطلاعات کاربر.
* حفاظت از منابع سیستم (شامل شبکه).
* فراهم کردن ایزوله کردن برنامه ها.

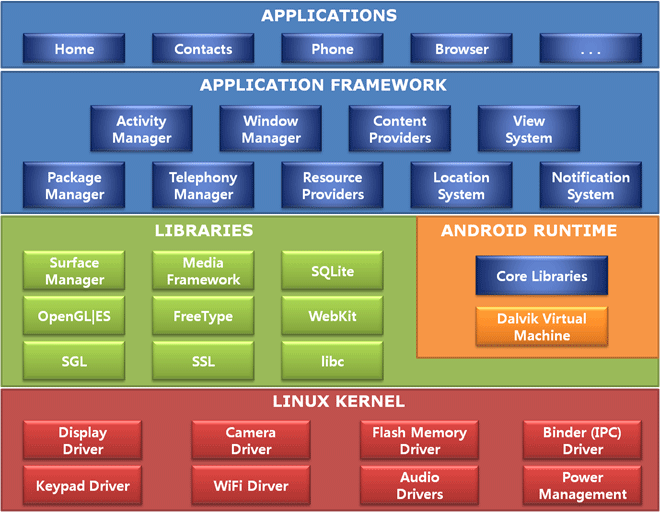
برای رسیدن به موارد نام برده، اندروید خصوصیتهای کلیدی زیر را معرفی میکند :

امنیت پرقدرت در سطح OS بواسطه کرنل لینوکس.

SandBox اجباری برنامه، برای تمام برنامه ها (SandBox یک مکانیزم امنیتی برای تست کدهای ناشناخته است).

* ارتباط بین پروسه ای امن
* امضای برنامه ها
* سطح دسترسی تعریف شده برای برنامه ها و اعطا شده به کاربر

در بخش پایین مسائل بالا به همراه خصوصیت های دیگری از پلتفرم اندروید را توضیح میدهیم. عکس1 خلاصه ای از ملاحظات و مولفه های سطحهای مختلف پشته ی نرم افزاری اندروید را نشان میدهد. در هر مولفه فرض شده که مولفه های زیرینش به درستی امن شده. به استثنای اجرای کد به عنوان root، تمام کدها در بالای کرنل لینوکس در Application SandBox محصور میشود.



# شکل 3- 6 پشته ی نرم افزاری اندروید

# 3-17 امنیت سطح کرنل و سیستم

در سطح سیستم عامل، پلتفرم اندروید امنیت کرنل لینوکس و نیز امنیت امکان ارتباط امن بین پروسه ای را برای فعال کردن ارتباط بین برنامه های درحال اجرا در پروسه های مختلف را مهیا میکند. این خصوصیات امنیتی در سطح سیستم عامل (OS)، تضمین میکند که حتا کدهای بومی هم در App SandBox اجرا شوند.

# 3-18 توصیه هایی برای امنیت بیشتر اندروید

روش هایی برای امنیت بیشتر، یافتن اپلیکیشن های مطمئن و اجتناب از ویروس ها در اندروید

این مطلب مناسب افرادی است که نگران امنیت اطلاعات گوشی های موبایل اندرویدی خود هستند. این که چه زمانی می توانند با خیال راحت اپلیکیشنی را دانلود کنند و به چه اپلیکیشن هایی باید شک کنند و دانلودشان نکنند. این مقاله می تواند به کاربران کمک کند تا دید درستی نسبت به نرم افزارهای گوشی، اطلاعات شخصی و حریم خصوصی شان داشته باشند. به اعتقاد ما، اندروید جزو پلتفورم های امن است. با کمی دقت، تلاش و دانش درست نسبت به تهدیدات بالقوه، کاربر می تواند با خیال آسوده و بدون نگرانی از گوشی خود استفاده کند.

لطفا توجه داشته باشید این مطلب، فقط بخشی از کارهایی است که کاربر باید برای امنیت بیشتر اطلاعات گوشی موبایل خود رعایت کند.

# 3-19  انواع برنامه های خطرناک

رایج ترین تهدیداتی که ممکن است از طرف اپلیکیشن های اندروید صورت گیرد، موارد زیر هستند:

1. مواقعی که اپلیکیشن کاربر را تحریک به اجازه دادن و تایید برای کاری می کند که اصلا نیازی به دسترسی به آن نیست. مانند دسترسی لازم برای ارسال اس ام اس یا برقراری تماس برای یک بازی یا برنامه ویرایش متن.
2. هنگامی که اپلیکیشن ها، کدهای مخرب خود را پشت اجازه نامه های قانونی و حق دسترسی های عادی پنهان می کنند.
3. هنگامی که اپلیکیشن موردنظر از کاربر می خواهد اطلاعات فردی و شخصی حساس خود، همچون شماره حساب مالی اش را برای نصب برنامه وارد کند.

هکرها و کِرَکرها برای نفوذ به گوشی های موبایل و سرقت اطلاعات آنها روش های متعددی دارند. این کاربر است که باید همیشه هوشیار باشد و دم به تله آنها ندهد.

 بدافزارها :بدافزار در واقع نوعی برنامه کامپیوتری و واژه ای جامع و فراگیر برای توضیح هر گونه برنامه مخرب و خطرناک است. بدافزار، همان طور که از نامش پیداست موجب ایجاد خسارت و آزار کاربران می شود. تعدادی از آنها علاوه بر آزار کاربران، از آنها سوءاستفاده های اطلاعاتی و مالی نیز می کنند. بدفزار، شامل جاسوس افزار، ویروس و هرگونه کلاهبرداری فیشینگ است. گاهی حتی مواردی که قبلا به آنها «ویروس» اطلاق می شد نیز در این دسته بندی قرار می گیرد. اما به طور کلی، بدافزار تهدیدات بسیار دقیق و قوی را شامل می شود.

جاسوس افزار:جاسوس افزار را از نامش نیز می توان حدس زد که چه وظیفه ای دارد. این نرم افزارها، دقیقا به کلمه جاسوس جامه واقعیت می پوشانند. یعنی نوعی برنامه یا نرم افزار هستند که بدون اطلاع کاربر، وارد سیستم او می شوند و اطلاعات آن را برای هکر سازنده اش ارسال می کنند. جاسوس افزار به طور مستقیم اثر تخریبی ندارد و کار آن جمع آوری اطلاعات و ارسال به شخص سوم است. اما گاهی این اطلاعات شامل رمزهای عبور و اطلاعات حساب مالی و کارت های اعتباری کاربر هستند.

##### فیشینگ: فیشینگ و جاسوس افزارها بسیار به هم شبیه هستند. در فیشینگ نیز کاربر فریب برنامه های قلابی را می خورد و اطلاعات مهم او برای شخص سوم ارسال می شود. تنها تفاوت فیشینگ و جاسوس افزار در این است که فیشینگ نوعی سرقت آنلاین است که قربانیانِ خود را، با ارسال ایمیل های جذاب و تشویق آنها به تماشای سایت های به ظاهر بی خطر، پیدا می کند. اما در همان هنگام اطلاعات فردی شان را به سرقت می برد. توجه داشته باشید که برخی سایت های فیشینگ به نظر خیلی واقعی می آیند. به طور مثال، از لوگو و طرح بانک ها و سایت های قابل اعتماد برای صفحه خود استفاده می کنند. البته اگر نگاهی دقیق تر داشته باشید، می توانید تقلبی بودن آنها را تشخیص دهید.

جاسوس افزارها خود را از دید کاربر مخفی می کنند، اما در فیشینگ، نرم افزار سارق خود را به کاربر نشان می دهد. ولی در هر دو حالت، اطلاعات کاربر بیچاره به سرقت می رود.

 ویروس :ویروس تعریف بسیار کلی دارد. این روزها، واژه «بدافزار» جایگزین «ویروس» شده است. ویروس در واقع به نرم افزاری گفته می شود که بدون اجازه کاربر وارد موبایل یا کامپیوتر او می شود و کنترل سیستم عامل را به دست می گیرد. یا حتی به آن آسیب می رساند. به طور مثال، می توان گفت ویروس ها از طریق ایمیل وارد سیستم کامپیوتری یا موبایل کاربر می شوند. آنها معمولا درون یک فایل ضمیمه شده قرار دارند که با گشودن یک صفحه HTML، فایل اجرایی برنامه یا حتی یک فایل متنی word می توانند فعال شوند. ویروس ها معمولا در پیام های ایمیل حرکت می کنند و با ارسال خودکار خود به فهرست آدرس هایی که در میل باکس قربانی وجود دارد، خود را تکثیر می کنند. ویروس های نیز همچون موارد ذکر شده در بالا یکی از تهدیدات اینترنتی جدی برای اندروید هستند.

 اسب تروجان: تروجان یکی از انواع خاص ویروس ها است. تروجان ها قابلیت تکثیر ندارند، از این رو در ردیف ویروس ها طبقه بندی نمی شوند. اما این قدرت را دارند که فایل های سیستم را پاک و در نحوه عملکرد سیستم اختلال ایجاد کنند یا حتی سیستم را از کار بیندازند. تروجان ها که به اسب تروا هم معروفند، عملکرد بسیار ساده و در عین حال خطرناکی دارند. آنها به صورت یک فایل موسیقی، بازی، تصویر گرافیکی زیبا یا هر چیز جذاب دیگر ظاهر می شوند. کاربر به خیالش یک برنامه ساده را باز می کند اما به محض اجرا کردن تروجان ها، ممکن است همه فایل های روی هارددیسک پاک یا به طور کلی هارد فرمت شود.

##### آگهی افزار یا Adware: آگهی افزار، همان طور که از نامش پیدا است برای انجام تبلیغات و آگهی های اینترنتی طراحی شده. اما این افزارها هویت تقریبا نامعلومی دارند. گاهی به آگهی افزارها، برنامه های آزاردهنده و مزاحم نیز گفته می شود. این نوع برنامه ها، اصولا تعداد زیادی آگهی و تبلیغات به جای نمایش وب سایت اصلی به کاربر نشان می دهند. البته آنها تقریبا خطر خاصی برای سیستم کاربر ندارند. اما باعث کاهش سرعت عملکرد سیستم، مصرف شدید پهنای باند اینترنت و ایجاد اختلال در اجرای برنامه های امنیتی می شوند.

گاهی آگهی افزارها با آگهی های واقعی در هم می شوند و امکان تشخیص آگهی واقعی وجود ندارد. به همین دلیل است که گفته می شود آگهی افزارها هویت نامعلومی دارند و شرکت های تولید کننده آنتی ویروس، دقیقا نمی دانند چگونه می توان با آگهی افزارها مقابله کرد.

##### وارز (Warez): وارز به معنای لغوی «انجمن» به نرم افزارهایی اطلاق می شود که قانون کپی رایت را رعایت نکرده اند. یعنی در واقع نرم افزارهایی هستند که بدون اجازه کپی شده اند. گاهی اوقات، فروم ها یا وب سایت های وارز اپلیکیشن های رایگان یا پکیج های اندرویدی را در اختیار کاربران قرار می دهند.

لطفا فریب اینگونه سایت ها را نخورید. برنامه ها و نرم افزارهای آن را دانلود و روی گوشی خود نصب نکنید. این فایل ها از برنامه نویس های حقیقی آنها به سرقت رفته است و این انجمن ها حقی برای ارائه آنها به دیگر کاربران ندارند.

اغلب اوقات، افرادی که این گونه انجمن ها را راه اندازی می کنند با سرقت نرم افزارها از جاهای مختلف، برای فوروم های خود آگهی نیز می گیرند و از طریق تبلیغات کسب درآمد هم می کنند.

در کنار همه این مسایل که به ضرر برنامه نویس های اصلی هست، این روش می تواند راهی برای نفوذ هکرها به سیستم های کامپیوتری و موبایلی کاربران نیز باشد. بیشتر سوءاستفاده کننده های اینترنتی، میان نرم افزارهای رایگان، برنامه هایی را می گذارند که در واقع یک بدافزار است و با ورود به موبایل کاربر می تواند اطلاعات او را به سرقت ببرد. حتی تعدادی از آنها، نرم افزارهایی را از اندروید مارکت می دزدند و با تغییر نام آن دوباره همان جا قرارشان می دهند.

اگر جزو کاربرانی هستید که همیشه از نرم افزارهای رایگان اندروید مارکت استفاده می کنند، احتمال خطر برای شما نیز وجود دارد. فروشگاه های معتبر برنامه های اندروید لیستی است که در پایین نام برده شده است. ترجیحا غیر از اینها به هیچ وب سایت دیگری اعتماد نکنید:

* Android Market گوگل
* AppStore آمازون
* SlideMe
* Archos AppsLib
* AndAppStore
* Market موتورولا (احتمالا فقط در آمریکای لاتین قابل دسترسی است)

به شما توصیه می کنیم برای حفظ امنیت خود، به غیر از این فروشگاه ها از جای دیگری برنامه دانلود یا خریداری نکنید. البته در مورد اپن سورس ها استثنا نیز وجود دارد. برنامه نویس های مستقلی نیز وجود دارند که اپلیکیشن ها و نرم افزارهای خود را برای فروش و دانلود در اینترنت به اشتراک می گذارند. اگر چه همچنان اصرار داریم که این برنامه ها نیز امنیت تضمین شده ای ندارند، اما نباید همه را به چوب انجمن های Warez راند. این اپلیکیشن ها شاید ویروس یا بدافزار نباشند، اما تضمینی هم برای امنیت آنها وجود ندارد.

برخی از محل های عرضه اپلیکیشن های رایگان متن باز (که وارز نیستند) شامل موارد زیر هستند:

* XDA Developers
* Googlecode
* GitHub

 درست همانند کامپیوترهای ویندوزی، تهدیدات موبایلی هم می توانند اطلاعات حساب مالی و کارت های اعتباری شما و همچنین فهرست مخاطبان تان را سرقت کنند. گزارش های اخیر نشان می دهند که بدافزارهای رایج این روزها، اپلیکیشن پیامک های پولی برای دزدیدن پول کاربران هستند. یکی دیگر از روش هایی که این بدافزارها می توانند به کاربر صدمه بزنند ضبط مکالمات تلفنی کاربر و ارسال آنها به یک هکر خرابکار است. البته خیلی نگران نباشید زیرا راه های گوناگونی برای محافظت در مقابل بدافزارها و دیگر تهدیدات امنیتی وجود دارد.

# 3-20 چگونه بدافزارها به دستگاه های اندرویدی راه پیدا می کنند

شیوه ورود بدافزارها به داخل دستگاه اندرویدی کاربر را مسیر حمله می گویند. این مسیر می تواند دانلود یک نرم‌افزار غیرامن از گوگل پلی یا دزدیده شدن گوشی موبایل باشد. اما رایج ترین راه نفوذ بدافزار به وسیله شما از طریق «مهندسی اجتماعی» است. به عبارت ساده تر، فریب دادن شما ساده ترین راه است.

برای هر اپلیکیشن معروف و اصلی، چند اپلیکیشن با نام تقریبا مشابه ساخته می شود تا کاربرانی که هنگام دانلود نرم‌افزار دقت کافی ندارند، گول بخورند و نرم‌افزار مخرب را به جای نسخه اصلی دانلود و روی گوشی یا تبلت خود نصب کنند. البته منظور این نیست که همه این نرم‌افزارها می توانند خطرناک و مخرب باشند اما بهتر است از این گونه نرم‌افزارها دوری کنید. شاید بتوان گفت بزرگ ترین مزیت سیاست بسته و محدود اپل این است که نرم‌افزارهای موجود در فروشگاه اینترنتی iOS، مشکلات چند نسخه ای بودن را ندارند.

 حتی اگر اپلیکیشن های اندرویدی هنگام نصب از کاربر اجازه‌نامه تقاضا کنند هم این مرحله از امنیت چندان کاربردی نیست و به نوعی می توان گفت زیادی هم هست. زیرا بیشتر اپلیکیشن ها – حتی نرم‌افزارهای خوب و سالم – همیشه چندین اجازه‌نامه از کاربر می خواهند و چه کسی زمان آن را دارد که تمام اپلیکیشن ها را ارزیابی کند تا مبادا مشکل امنیتی داشته باشد؟ تقریبا بهترین روش برای امنیت بیشتر این است که مطمئن شوید برنامه ای که دانلود کرده اید نسخه کپی شده خطرناک نیست و نسخه اصلی است.

# 3-21  ترفندهای ساده برای محافظت از امنیت موبایل

نخستین روش دفاع در هر کدام از شیوه نامه های امنیت سایبری، اصلاح رفتار خودمان است. به طور مثال، تا حد امکان اطلاعات شخصی بسیار کم و محدودی را در تلفن همراه خود نگهدارید. یا مثلا رمزهای عبور و اطلاعات کارت های اعتباری خود را در فایل های بدون رمز نگه ندارید.

همچنین، هنگامی که مرورگر سیستم از شما می خواهد تا رمزعبور را برای تان ذخیره کند یا خیر، شما همیشه گزینه خیر را انتخاب کنید. به جای آن می توانید از راه‌حل امن تری همچون LastPass استفاده کنید. اندروید راه های فیزیکی مختلفی نیز برای محدود کردن دسترسی ها دارد. به طور مثال، می توانید میان گزینه های Screen Lock در بخش امنیت در قسمت تنظیمات گوشی جست‌وجو کنید. در این قسمت می توانید برای گوشی خود پین کد، رمزعبور یا یک الگو (Pattern) تعریف کنید تا هر کسی دسترسی به داخل گوشی نداشته باشد.

البته این را هم در نظر داشته باشید که فردی که نتواند به راحتی وارد برنامه های گوشی بشود، ممکن است از طریق یو‌اس‌بی به اطلاعات آن دسترسی پیدا کند. برای دفاع در برابر چنین نفوذی، از گزینه رمزگذاری داخلی برای رمزدار کردن همه اطلاعات و تنظیمات گوشی استفاده کنید. پنهان و رمزدار کردن همه قسمت های گوشی حدود یک ساعتی زمان نیاز دارد، پس باید از شارژ بودن باتری گوشی اطمینان حاصل کنید یا آن را به برق بزنید که همه کارها با موفقیت انجام شوند.

شما همچنین باید حواس تان جمع باشد که چه نرم‌افزاری را از گوگل پلی دانلود می کنید. همان طور که پیش از این نیز گفتیم، مراقب اپلیکیشن های مخرب باشید که کپی و مشابه نسخه های اصلی اپلیکیشن ها هستند. برای محافظت در برابر این تهدیدها، شرکت سیمانتک – بزرگ ترین شرکت تولیدکننده نرم افزارهای امنیتی – یک ارزیابی از تعداد نرم‌افزارهای آلوده به بدافزار موجود در گوگل پلی عرضه کرده است. بر اساس این آمار، از میان ۱۲۰۴۷۲ اپلیکیشن سرگرمی موجود در گوگل پلی، فقط دو اپلیکیشن مخرب یا بدافزار وجود داشت. موردی که در اینجا باید به آن توجه داشته باشید، فعال کردن گزینه «منابع ناشناخته» در تنظیمات امنیت است که به شما اجازه می دهد هر فایل APK را دانلود و نصب کنید. شما باید همیشه دستگاه خود را با جدیدترین آپدیت سخت‌افزار به روز نگه دارید.

# 3-22 پیشنهاد برای استفاده از ضد بدافزار

تقریبا همه پیشگیری های ذکر شده در بالا، امنیت شما را در برابر تهدیدات بدافزارها و برنامه های مخرب حفظ می کنند. اما اگر همچنان تمایل دارید که خیال تان حسابی از امنیت گوشی جمع باشد، می توانید اپلیکیشن ضد بدافزار روی وسیله خود نصب کنید. به این ترتیب، احتمال آلوده شدن گوشی به فایل های مخرب بسیار کاهش پیدا می کند.

در بررسی جدید سایت av-test.org نشان می دهد، آنتی ویروس ها و ضد بدافزارهای زیر بیش از ۹۰ درصد در دفاع از ابزارها در برابر تهدیدات اینترنتی موفق بوده اند.

* avast! Mobile Security
* Lookout Security & Antivirus
* Dr Web Anti-virus
* F-Secure Mobile Security
* IKARUS mobile.security
* Kaspersky Mobile Security
* Zoner AntiVirus
* McAfee Antivirus & Security
* MYAndroid Protection Antivirus
* NQ Mobile Security & Antivirus

# 3-23 امنیت اندروید را جدی بگیرید

قفل کردن گوشی توسط‌pattern :همه گوشی‌های امروزی امکان قفل کردن گوشی توسط pattern را دارند که امكان استفاده از این ابزار فقط برای صاحبان گوشی وجود دارد. هرچند روش‌هايی برای دور زدن pattern lock وجود دارد، اما فقط هکرهای ماهر توان عبور از آن را دارند و بسیاری از افراد امکان عبور از این سد امنیتی را ندارند. بنابراین توصیه می‌شود حتما از یکی از روش‌های قفل کردن گوشی استفاده شود تا یک سد امنیتی برای گوشی ایجاد شود.

 خاموش کردن بلوتوث و وایرلس‌: هنگامی که نیازی به استفاده از وایرلس و بلوتوث ندارید حتما آنها را خاموش کنید؛ چراکه هکرها توسط ابزارهای خاصی به scan کردن دستگاه‌های اطراف به‌وسیله بلوتوث یا وایرلس اقدام کرده و توسط روش‌ها و ابزارهای خاصی به انجام حمله‌های متعدد اقدام کرده و سعی خواهند کرد در دستگاه‌ها نفوذ کنند. البته موفقیت‌آمیز بودن این روش‌ها نیازمند مهارت و تجربه بسیار بالا است و تعداد بسیار کمی از هکرها توان انجام آن را دارند، اما برای حفظ امنیت بیشتر توصیه اکید می‌شود در صورت استفاده نكردن از تکنولوژی‌های ارتباطی روی گوشی، آنها را غیرفعال کنید.

خروج از سایت‌های مالی پس از انجام فعالیت: اگر برای انجام فعالیت‌های مالی از گوشی استفاده می‌کنید، توصیه می‌شود حتما پس از انجام فعالیت از سایت مورد نظر کاملا خارج شده یا اصطلاحا log out كنيد؛ چراکه برخی از کاربران بدون log out کردن، پنجره سایت مربوطه را می‌بندند که باعث خروج کامل از آن نمی‌شود و می‌تواند مشکلات امنیتی را برای کاربر به دنبال داشته باشد.

 توجه دقیق به permission‌های اخذشده توسط نرم‌افزار: هر نرم‌افزار به هنگام نصب شدن در گوشی از کاربر برخي مجوزها را درخواست می‌کند که کاربر قبل از نصب باید آنها را تایید کند. متاسفانه اکثر کاربران بدون توجه به مجوزهای اخذشده توسط نرم‌افزار، آن را نصب می‌کنند. توجه نكردن به صدور مجوز برای برنامه‌ها می‌تواند خطرات بسیار جدی را برای گوشی و کاربر به همراه داشته باشد؛ چراکه می‌تواند به قسمت‌ها و امکانات مختلف گوشی و اطلاعات کاربر، دسترسی پیدا و آن را منتشر كند. توصیه می‌شود قبل از نصب هر برنامه‌ای لیست دسترسی‌های هر برنامه را ارزیابی و در‌صورتی‌که مجوزهای درخواستی فراتر از نیاز برنامه بود از نصب آن خودداری کنید.

غیرفعال کردن GPS :تنها در مواقعی که نیاز به مکان‌یابی دارید قابلیت GPS را فعال کنید؛ چراکه فعال بودن پیوسته GPS در گوشی خطر ارسال موقعیت جغرافیایی کاربر توسط برنامه‌های مشکوک در اینترنت را به دنبال خواهد داشت که یک نوع جاسوسی محسوب می‌شود. ماهیت عملکردی برخی از نرم‌افزارها برخلاف ظاهر کاربردی آنها حالت جاسوسی دارد که بدون اجازه کاربر به ارسال موقعیت مکانی او توسط اینترنت اقدام می‌کنند.

استفاده از Firewall‌ :نصب بودن یک دیواره آتش قوی در موبایل این امکان را به کاربر می‌دهد که تمامي اطلاعات دریافتی یا ارسالی در گوشی را مانیتورینگ کند یا امکان دسترسی یک برنامه به اينترنت را محدود کند و همچنین از نفوذ افراد سودجو به گوشی از پورت‌های مختلف جلوگیری کند.

 رمزگذاری روی فایل‌های متنی حساس :بسیاری از کاربران در گوشی خود به نوشتن یاد‌داشت اقدام می‌کنند که می‌تواند حاوی اطلاعات محرمانه و شخصی آنان باشد؛ بنابراین لازم است تا از آن محافظت کنند. یکی از اقدامات مفید در این زمینه، استفاده از نرم‌افزارهایی است که مانند گاوصندوق عمل می‌کند و کاربر می‌تواند فایل‌های متنی ایمن ایجاد و روی آن رمز بگذارد و فقط با داشتن رمز عبور تعریف‌شده می‌تواند به یادداشت‌های خود دسترسی داشته باشد. اگر جزو آن دسته از کاربرانی هستید که در گوشی خود یادداشت‌های شخصی و مهمی دارید توصیه می‌شود حتما از این نرم‌افزارها استفاده کنید.

 حذف اطلاعات از راه دور: یکی از اقداماتی که هر کاربر باید انجام دهد، استفاده از ابزارهایی است که توسط آنها می‌توان از راه دور به حذف ایمن اطلاعات موجود در گوشی اقدام كرد. این کاربرد وقتی اهمیت دارد که گوشی گم یا سرقت می‌شود و کاربر بیش از هر چیزی نگران اطلاعات داخل گوشی است که توسط این ابزارها می‌تواند از راه دور به حذف آنها اقدام كند.

**اضافه کردن لایه ای جدید به سیستم امنیت اندروید :**یکی از کارشناسان ارشد سیستم های موبایل اندرویدی  چندی پیش سرویسی به نام Bouncer در زمینه امنیت بیشتر سیستم عامل اندروید معرفی و عرضه کرده است. سرویس بانسر به صورت خودکار همه اپلیکیشن های اندروید مارکت را به منظور یافتن بدافزارهای مخفی و غیرقابل تشخیص، اسکن می کند. روند اسکن خودکار این نرم افزار، در گشت زنی کاربر در  فروشگاه اینترنتی اندروید یا نیاز برنامه نویس ها برای ورود به فرآیند تایید اپلیکیشن ها، هیچ گونه خللی ایجاد نمی کند.

این سرویس برای جلوگیری از به خطر افتادن کاربر، هنگام ورود به اندروید مارکت، همه نرم افزارهای جدید، نرم افزارهای موجود در مارکت و همچنین حساب های کاربری برنامه نویس ها را مورد بررسی قرار می دهد. روند کار این سرویس نیز به این ترتیب است که: هنگامی که یک اپلیکیشن آپلود می شود، بانسر بلافاصله برای پیدا کردن بدافزار، جاسوس افزار و تروجان های شناخته شده آن را مورد بررسی قرار می دهد. سپس به رفتارهای اپلیکیشن توجه می کند که ببیند آیا رفتاری غیرمعمول در مقایسه با دیگر اپلیکیشن های اسکن شده دارد یا خیر. این کار را تا جایی ادامه می دهد که اگر اپلیکیشن موردنظر برای امنیت سیستم عامل خطرناک بود، بلافاصله فعالیت  آن را مسدود کند.

طراح این سرویس در این رابطه می گوید: «ما  تقریبا همه اپلیکیشن ها را در زیرساخت سیستم ابری گوگل اجرا و طریقه فعالیت آن را روی دستگاه های اندرویدی شبیه سازی می کنیم تا رفتارهای تخریب گرایانه و مخفی نرم افزارها را پیدا کنیم.» او همچنین اظهار داشت:«بعلاوه، ما حساب های جدید برنامه نویس ها را نیز بررسی می کنیم تا در صورت وارد کردن بدافزار به سیستم، دیگر اجازه فعالیت دوباره در اندروید مارکت را نداشته باشند.»

**کاهش میزان دانلود بدافزارها :**سرویس بانسر در حال حاضر در فروشگاه اینترنتی اندروید فعالیت دارد و در نتیجه آن و در مقایسه با دو نیمه سال گذشته میلادی، میزان دانلود بدافزارها از اندروید مارکت حدود 40 درصد کاهش داشته است. این کاهش چشمگیر درست هنگامی روی داد که شرکت های تولید کننده و فروشنده های نرم افزارهای امنیتی و ضد ویروس اعلام کرده بودند که تعداد بدافزارهای فروشگاه اینترنتی اندروید در حال افزایش بی رویه است.

از آنجایی که نمی توان جلوی فعالیت هکرها و نویسنده های ویروس ها و بدافزارها را گرفت، بنابراین بهترین راه برای امنیت این است که پیش از دانلود اپلیکیشن از ویروسی نبودن آن اطمینان حاصل کنیم. این ارزیابی به طور قابل ملاحظه ای میزان امنیت سیستم های اندرویدی را افزایش می دهد.

# 3-24 اندروید، قدرت نفوذ بدافزارها را کاهش می دهد

علاوه بر طراحی سرویسی جدید برای جلوگیری از نفوذ بدافزارها، گروه همکاری هیروشی لاخی‌میِر، سیستم عامل  اندروید را به منظور کاهش درصد نفوذ بدافزارها از نو طراحی کرده اند. در نمونه های کامپیوتری، بدافزارها به راحتی می توانند اطلاعات کاربر را به دست بیاورند و از آن سوءاستفاده کنند. اما گروه همکاری هیروشی لاخی‌میِر با توجه به این موضوع، سیستم عامل اندروید را برای اتصال به اینترنت طراحی کرده اند.

# 3-25 [هک کردن گوشی های اندروید](http://laitec.ir/?p=11342)

هک کردن گوشی های اندرویدی که به اصطلاح روت (Root) کردن نامیده می شود برای افراد تازه کار کمی دشوار و پیچیده به نظر می رسد. اما وقتی گوشی خود را روت می کنید از امکانات بیشتر و برنامه های جانبی متنوع می توانید بهره بگیرید.

تنظیمات و امکانات پیش فرضی که روی گوشی های هوشمند اندروید وجود دارند کم یا نامناسب نیستند. اما برخی کاربران از برنامه های موجود خسته می شوند و ترجیح می دهند اپلیکیشن های جدید و تنظیمات متفاوتی را تجربه کنند. برای این منظور هم به روت کردن گوشی نیاز دارد.

# 3-26 روت کردن چیست؟

روت کردن به طور مختصر یعنی روندی که به واسطه آن کاربر تنظیمات گوشی یا تبلت اندرویدی خود را از حالت کارخانه ای خارج و همه چیز را به سلیقه شخصی خود تغییر می دهد. این کار دقیقا همان جیل‌برک کردن سیستم عامل iOS است. این کار اصولا برای دور زدن محدودیت های کارخانه ای است که روی محصولات اعمال می شوند.پس از روت کردن می توانید برنامه هایی که تنظیمات پیش فرض گوشی اجازه نصب آنها را نمی دهد روی گوشی یا تبلت نصب کنید.یکی از رایج ترین دلایل روت کردن اندرویدی ها جایگزینی سیستم عامل با ROM، نسخه جدیدتر سیستم عامل و کنترل داشتن روی جزئیات گوشی است. در روند روت کردن این کار فلش کردن ROM گوشی معنا می دهد.گوشی های مختلف به روش های گوناگون روت می شوند. البته باید این را نیز در نظر داشته باشید که روت کردن باعث از بین رفتن گارانتی یا وارانتی گوشی می شود.

# 3-27 چرا گوشی را Root کنیم؟

روت کردن گوشی چند دلیل منطقی دارد. بارزترین و مهم ترین دلیل آن، حذف اپلیکیشن ها و بازی هایی است که به آنها نیازی ندارید و اپراتور یا سازنده بالاجبار روی گوشی هوشمند خود آنها را نصب کرده است. با این کار علاوه بر اینکه از دست این برنامه ها خلاص می شوید، فضای ذخیره بیشتری نیز در اسمارت فون باز می شود که می توانید استفاده مناسب تری از آن داشته باشید.از دیگر دلایل روت کردن، آپ دیت های سریع تر پلتفرم گوشی هوشمند است. هنگامی که گوگل نسخه جدیدی از سیستم عامل خود را معرفی و عرضه می کند، تا زمانی که بخواهد نسخه رسمی آن برای گوشی شما عرضه شود هفته ها و گاهی حتی ماه ها طول می کشد. با روت کردن گوشی می توانید هر زمانی که پلتفرم جدید عرضه شد، آن را دانلود و روی گوشی نصب کنید. با این کار می توانید همان گوشی خود را برای سال ها داشته باشید و بی جهت برای خرید گوشی جدید هزینه اضافه نکنید.یکی دیگر از مزیت های روت کردن این است که می توان به واسطه آن نسخه پشتیبان کاملی از گوشی و برنامه های داشت و با تغییر تنظیمات پیش فرض باعث بیشتر شدن عمر باتری شد.

# 3-28 اپلیکیشن های ارزشمند و مهم

پس از نصب رام دلخواه، می توانید روی گوشی هوشمند خود انواع اپلیکیشن ها و بازی های جدید و متنوع نصب و اجرا کنید. اگر به رابط کاربری رام جدید علاقه ای ندارید می توانید اپلیکیشنی نصب کنید تا قابلیت های جدید به گوشی هوشمند اندرویدی شما اضافه کند. از جمله این نرم افزارها باید به ROM Toolbox Pro، Titanium Backup، Touch Control، Cerberus anti-theft و SetCPU اشاره کرد.کاربرانی که قصد فلش کردن رام به روش های پایه را دارند، توصیه می کنیم با ROM Manager این کار را انجام دهند. این ابزار کمک می کند تا نسخه های پشتیبان و ریکاوری ها، نصب رام و قابلیت های دیگر را به خوبی و بسیار راحت مدیریت کنید. این اپلیکیشن رایگان است اما نسخه پولی آن، نوتیفیکیشن آپ‌دیت ROM، دانلودهای شبانه رام، بک‌آپ گیری خودکار و … نیز دارد.

# 3-29 [راه هایی برای محافظت از دستگاه اندرویدی در برابر ویروس](http://www.bartarinha.ir/fa/news/188991/%D8%B1%D8%A7%D9%87-%D9%87%D8%A7%DB%8C%DB%8C-%D8%A8%D8%B1%D8%A7%DB%8C-%D9%85%D8%AD%D8%A7%D9%81%D8%B8%D8%AA-%D8%A7%D8%B2-%D8%AF%D8%B3%D8%AA%DA%AF%D8%A7%D9%87-%D8%A7%D9%86%D8%AF%D8%B1%D9%88%DB%8C%D8%AF%DB%8C-%D8%AF%D8%B1-%D8%A8%D8%B1%D8%A7%D8%A8%D8%B1-%D9%88%DB%8C%D8%B1%D9%88%D8%B3)

همیشه وقتی صحبت از ویروس‌ها و نرم‌افزارهای مخرب دستگاه‌های موبایل می‌شود مقداری ترس، عدم اطمینان و شک وجود دارد. مطمئناً افراد خیلی باهوشی وجود دارند که شاید دست به هر کاری بزنند تا به اطلاعات گوشی شما دسترسی پیدا کنند و قسمت‌های جالب آن را برای اهداف مخرب خود استفاده کنند.

حقیقت این است که آن‌ها برای انجام یک حمله‌ی موفق باید خیلی بیشتر از آن مقدار که شما برای تأمین امنیت کارهایی را انجام می‌دهید تلاش کنند. اما در این میان چند کار ساده وجود دارد که می‌توانید برای تأمین امنیت خود در حین لذت بردن از گوشی‌تان انجام دهید و تا وقتی که این مراحل را فراموش نکنید خطری شما را تهدید نمی‌کند. با ما همراه باشید تا همین چند کار ساده را با هم مرور کنیم.

قبل از لمس نگاه کنید.

اگر بدانید که امروزه چقدر دسترسی‌های غیرمجاز به حساب‌های کاربری اصلاً نیازی به اکسپلویت مستقیم سرویس‌ها برای دسترسی به اطلاعاتتان ندارد تعجب خواهید کرد. مشخص شده که ضعیف‌ترین نقطه در این زنجیره خود کاربر است. در اینجا این کاربر شما هستید.

اگر صفحات پاپ آپ یا لاگین جعلی بتوانند شما را گول بزنند تا اطلاعات مهم خود را وارد کنید، دیگر نیاز به هک کردن هیچ‌چیز نیست چراکه شما هدفمند این اطلاعات را تقدیم افراد سودجو کرده‌اید. این اطلاعات به رباتی داده می‌شود که به جای شما سعی می‌کند به هر چیزی وارد شود و بعد دوستانتان مثلاً در سایت توییتر پیام‌هایی مزاحم حاوی لینکی که در مرحله اول برای شما نمایش داده شده را دریافت می‌کنند.

متأسفانه یک راه خودکار یا شخص ثالثی برای جلوگیری از این مدل مهندسی اینترنت وجود ندارد. اگر می‌خواهید دستگاه و حساب‌هایتان را از این‌گونه سوءاستفاده‌ها در امان نگه دارید باید قبل از لمس صفحه، خوب نگاه کنید. هیچ‌کس یک دستگاه پلی‌استیشن ۴ ندارد که اگر روی لینکش کلیک کنید و به فیس‌بوک خود وارد شوید آن را به شما بدهد و هیچ راهی برای خلاص شدن از چربی‌های دور شکم وجود ندارد که نیاز به نصب برنامه‌ی خاصی داشته باشد که در گوگل‌پلی استور نیست. دقیقاً مثل کامپیوتر باید مراقب کارهایی که انجام می‌دهید باشید.

قسمت Unknown sources را غیرفعال کنید

این قسمت اولین مرحله از محافظت از دستگاه‌هایتان در دنیای موبایل است. هر گوشی اندرویدی یک قابلیت دارد که در آن از نصب برنامه‌هایی خارج از گوگل‌پلی جلوگیری می‌کند.

در بیشتر جاها این قابلیت بسیار مفید است. با این روش می‌توانید به چیزهای هیجان‌انگیز نظیر کافه‌بازار، مایکت و دیگر اپ‌استورهای مطمئن ایرانی دسترسی پیدا کنید و این دقیقا یکی از چیزهایی است که به اندروید کمک می‌کند تا باز و انعطاف‌پذیر باقی بماند اما متأسفانه تعداد اندکی از برنامه‌ها از شما می‌خواهند که فراموش نکنید بعد از نصب برنامه موردنظر از این اپ‌استورها باید دوباره گزینه موردنظر را غیرفعال کنید. مهم نیست که چقدر فکر می‌کنید زرنگ هستید، باز گذاشتن این در برای گوشی یا تبلت هیچ‌گاه نباید اتفاق بیفتد و هرکسی باید این کار را انجام دهد.

به قسمت تنظیمات دستگاه خود بروید، به قسمت Security وارد شوید و گزینه‌ای که دارای Unknown sources است را پیدا کنید. تیک این گزینه را بردارید. بعداً گوشی دوستتان را هم برداشته و این گزینه را برایش حذف کنید و او را به خاطر انتخاب نکردن قفل برای گوشی سرزنش کنید.

از برنامه‌های غیرقانونی دوری کنید

دلایل خوبی برای نصب برنامه‌هایی که در گوگل پلی استور نیستند وجود دارند اما شاید نه به اندازه گذشته. گوگل به سختی تلاش کرده تا فضایی را برای تست کاربران، برای کمپانی‌هایی که می‌خواهند به تست ویژگی‌های برنامه‌های بتای خود بپردازند به وجود بیاورد. برنامه‌های قانونی وجود دارند که به نقض قوانین گوگل با تبلیغ اپ استورهای خودشان یا ارائه محتوایی که گوگل با آن‌ها مخالف است (مثل محتوای مخصوص بزرگ‌سالان) می‌پردازند؛ اما به‌جز این برنامه‌ها چیز دیگری نیست که بخواهید به آن دسترسی داشته باشید و در گوگل پلی استور وجود نداشته باشد.

تأمین امنیت دستگاه روت شده یک غول مرحله آخر کاملاً جداست که بعداً به آن می‌پردازیم؛ اما برای اکثریت کاربران تنها چیزی که لازم است بدانند این است که هرگز خارج از گوگل پلی استور به نصب برنامه‌ها نپردازند مگر اینکه ۱۰۰ درصد مطمئن باشند خطری تهدیدشان نمی‌کند.

مشخص شده افرادی که برنامه‌ها را از توسعه‌دهندگان زحمت‌کش می‌دزدند و آن‌ها را مجانی برای شما در اپ استور خود قرار می‌دهند قابل اعتمادترین افراد دنیا نیستند. عجیب است نه؟ شاید این اپ استورها برای اینکه قبل از خرید یک برنامه آن را دانلود کرده و تست کنید مناسب باشند اما برای بیشتر این اپ استورها هیچ قانون و حد وسطی وجود ندارد.

شاید این برنامه‌ها دستکاری شده باشند یا فقط یک نرم‌افزار مخرب بوده و با عنوان دیگری نام‌گذاری شده باشند و وقتی که این برنامه‌ها به گوشی شما برسند دیگر خیلی دیر شده. بهترین کار برای جلوگیری این است که فقط از این مارکت‌ها دور بمانید و به دنبال نسخه مجانی برنامه‌های دلخواهتان نباشید. شما بهتر از آن هستید.

دسترسی‌هایی که در هنگام نصب برنامه نمایش داده می‌شود را به دقت بخوانید

هر برنامه‌ای را که بر هر دستگاه اندرویدی نصب کنید به شما می‌گوید که دقیقاً به چه قسمت‌هایی از سیستم‌عامل نیاز خواهد داشت به‌علاوه اطلاعات شخصی شما. این اطلاعات بین زمانی که تصمیم می‌گیرید برنامه‌ای را نصب کنید و زمانی که روی دستگاهتان نصب می‌شود به شما نشان داده خواهد شد و زمانی برای بررسی اطلاعات و دسترسی‌های موردنیاز برنامه خواهید داشت.

درحالی‌که می‌توان با این اجازه‌های دسترسی مثل قوانین نصب یک برنامه‌ی جدید در کامپیوترهای سنتی رفتار کرد و زود از آن‌ها رد شد، ده ثانیه‌ای که صرف بررسی آن‌ها می‌کنید می‌تواند به شما در جلوگیری از نصب بدافزارها و ویروس‌ها کمک کند. این ده ثانیه از زندگی شماست. اجازه‌های دسترسی برنامه‌ای را که می‌خواهید نصب کنید بخوانید و از پرسیدن سؤال نترسید. البته برای هرکدام از این اجازه‌ها و دسترسی‌ها دلیل خوبی وجود دارد، اما بهتر است که علت آن‌ها را برای مطمئن شدن بدانید.

یک آنتی‌ویروس خوب ضرری نخواهد داشت اما لزوماً کمکی هم نمی‌کند

اهمیتی ندارد از چه سیستم‌عاملی استفاده می‌کنید چیزی به اسم حفاظت کامل در مقابل ویروس‌ها، حملات فیشینگ و نرم‌افزارهای مخرب و جاسوسی و در موارد حاد اکسپلویت‌هایی که به گوشی‌تان صدمه می‌زنند وجود ندارد. ما هر چیزی از ایستگاه‌های شارژ یو‌اس‌بی مثلاً در یک فروشگاه که کافی است تصمیم بگیرید گوشی‌تان را با آن‌ها شارژ کنید تا کد مخربی را در آن اجرا کنند گرفته تا برنامه بازی شطرنج که دقیقاً دو هفته صبر می‌کند تا از شما بپرسد آیا می‌خواهید خانم‌های جذابی را در محدوده‌تان هستند ملاقات کنید دیده‌ایم.

درست است با برنامه‌ای که گوگل در گوشی‌تان جاسازی کرده در مقابل بسیاری از شیاطین این حیطه از شما محافظت خواهد شد، اما ضرر ندارد از یک جفت چشم اضافی برای محافظت بیشتر در مقابل مشکلات استفاده کنید.

با استفاده از یک برنامه آنتی‌ویروس مشهور چند چشم اضافی برای مراقبت از خودتان دارید. این شرکت‌ها محققان امنیتی را استخدام می‌کنند تا به شما در امن نگه داشتن هویتتان در هنگام وب گردی، تماس‌های تبلیغاتی مزاحم و امنیت‌های قوی‌تر از راه دور مثل زمانی که گوشی دزدیده یا گم شده کمک کنند. البته نمی‌توانید انتظار کمک زیاد برای برنامه‌هایی که درست کار نمی‌کنند داشته باشید. اگر به تمام ویژگی‌هایی که تمام برنامه‌های موجود در اینترنت هستند نگاهی بیندازید مطمئناً چیزی را که مناسب حالتان باشد پیدا خواهید کرد پس تصمیم با شماست که ببینید این ویژگی‌ها قابلیت استفاده از آن برنامه را دارند یا خیر.

مهم است به خاطر داشته باشید که چقدر تنها خود گوشی، مخصوصاً برنامه‌های گوگل و سرویس‌های آن به تنهایی امنیت گوشی شما را تأمین می‌کنند. ابزارهایی وجود دارند که به عنوان بخشی از سرویس‌های گوگل به صورت منظم گوشی‌تان را چک می‌کنند حتی می‌توانند در صورت لزوم اگر برنامه‌ای برایتان خطرناک باشد آن را از گوشی‌تان حذف کنند؛ اما به این معنی نیست که هر کاری که خواستید بکنید و نگران نتایجش نباشید. خودتان را امن نگه دارید و تکنولوژی که در دست دارید لذت ببرید.

اینها اقدامات ساده‌ای بود که برای حفظ امنیتی گوشی اندرویدی خود به انجام آنها و رعایت انها نیاز دارید. مطمئنا خودتان دریافته‌اید که مهم‌ترین چیز خود شما هستید!

# فصل چهارم

# نتیجه گیری

Android به زبان ساده سيستم عاملي است براي دستگاه هاي موبايل و گوشي هاي هوشمند که توسط بيش از 30 کمپاني معروف پشتيباني مي شود. آندرويد اوپن سورس است و توسعه دهندگان مي توانند با استفاده از Android SDK برنامه هاي مختلفي براي اين سيستم عامل بنويسند. در واقع آندرويد بستري را فراهم مي کند تا برنامه نويسان بتوانند هرچه سريعتر و بهتر برنامه هايي بسازند که از تمام ويژگي هاي يک گوشي هوشمند استفاده کند. آندرويد به معناي واقعي “ باز (Open) “ است، يعني برنامه نويس مي تواند از تمام قدرت يک تلفن همراه استفاده کند. آندرويد امکان استفاده از توابع داخلي گوشي موبايل همچون شماره گيري، فرستادن SMS يا استفاده از دوربين گوشي را به برنامه نويسان مي دهد تا بتوانند اپليکيشن هاي قدرتمند و کاربردي براي کاربران بسازند.

تمام برنامه ها براي آندرويد يکي اند. آندرويد فرقي ميان يک برنامه third-party و توابع هسته سيستم عامل در اجرا نمي گذارد و هر دو مي توانند دسترسي مساوي به قابليت هاي گوشي داشته باشند. گوشي هايي که سيستم عامل آندرويد را خواهند داشت به کاربرشان اجازه مي دهند تا از تمام قابليت هاي يک گوشي هوشمند بهره ببرند. کاربران اين گوشي ها به معناي واقعي مي توانند دستگاه خود را بر اساس سليقه ي خود تغيير دهند و محيط سيستم عامل گوشي خود را سفارشي و شخصي سازي کنند. حتي کاربران مي توانند براي گوشي تعيين کنند که عکس هايشان با چه برنامه اي باز شود.

گوشی های هوشمند به سرعت در حال تبدیل شدن به یک پلت فرم محاسباتی غالب هستند. موانع کم ورودی برای توسعه دهندگان نرم افزار خطر امنیتی برای کاربران نهایی را افزایش می دهد. در این مقاله، ما دیکامپایلر DED برای برنامه های آندروید شرح داده و از کد منبع جدا شده برای انجام مطالعه گسترده هر دو عملکرد خطرناک و آسیب پذیری استفاده کردیم. در حالی که یافته های در معرض شناسه های تلفن و محل ما با مطالعات قبلی مطابقت دارد، چارچوب تجزیه و تحلیل ما نه تنها اجازه می دهد تا وجود قابلیت های خطرناک را مشاهده کنیم، بلکه چگونگی رخ دادن آن در چارچوب برنامه را نیز نشان می دهد.

حرکت رو به جلو، ما DED و مشخصات تجزیه و تحلیل مان را پیش بینی می کنیم، به عنوان فن اوری فعال که درهای جدیدی برای صدور گواهینامه برنامه باز خواهد کرد. با این حال، ادغام این فن آوری ها با فرآیند صدور گواهینامه نرم افزار به غلبه بر چالش های تدارکاتی و فنی نیاز دارد. کار آینده ما این چالش ها، و گسترش تجزیه و تحلیل ما به مناطق جدید، از جمله نصب و راه اندازی نرم افزار، JNI مخرب و فیشینگ را در نظر خواهد گرفت.

بدین ترتبت نتیجه میگیریم که سیستم عامل اندروید یکی از معرف ترین و کارآمد ترین سیستم عامل های موجود در جهان می باشد که از زمان پیداش تاکنون علی رغم نقاط قوت و و ضعف در ویرایش های مختلف آن،همواره در مسیر تکاملی خود سعی بر کاهش نقاط ضعف و رسیدن به امکانات و خدمات مطلوب کاربران کرده است.

بدین ترتبت نتیجه میگیریم که سیستم عامل اندروید یکی از معرف ترین و کارآمد ترین سیستم عامل های موجود در جهان می باشد که از زمان پیداش تاکنون علی رغم نقاط قوت و و ضعف در ویرایش های مختلف آن،همواره در مسیر تکاملی خود سعی بر کاهش نقاط ضعف و رسیدن به امکانات و خدمات مطلوب کاربران کرده است.

# منابع

تمامی منابع و مراجعی که این مقاله از روی انها تنظیم گردیده وب سایت ها و کتاب های الکترونیکی می باشند

سایت های اینترنتی:

1. وب سایت رسمی اندروید www.android.com
2. انجمن کامپیوتر www.P30world.com
3. انجمن فناوری اطلاعات تبیان www.Tebyan.net
4. سایت خبری فراسان [www.farasun.wordpress.com](http://www.farasun.wordpress.com)
5. ایجل، ام. کروگل، سی. کردا، ای. و ویجنا، جی. PiOS: تشخیص نشت حریم شخصی در نرم افزار IOS. در مجموعه مقالات همایش امنیت سیستم توزیع شده و شبکه (2011).
6. انک،دبلیو. گیلبرت،پی. چون،بی.جی. کاکس،ال.پی. یونگ،جِی. مک دانیال،پی. و شیز،اِی.ان. مقالات آلوده شده: اطلاعات جریان سیستم ردیابی برای نظارت پنهانی بیدرنگ بر گوشی های هوشمند. مجموعه مقالات همایش USENIX در طراحی و پیاده سازی سیستم های عامل (2010).
7. انک،دبلیو. اُکتا،دی. مک دانیال،پی و چادوری،اس. ررسی برنامه امنیتی آندروید . انجمن. عطف NASTR-0144-2011، مرکز تحقیقات امنیت و شبکه، گروه علوم کامپیوتر و مهندسی، دانشگاه ایالتی پنسیلوانیا، پارک دانشگاه، PA، ایالات متحده آمریکا، ژانویه 2011.
8. انک،دبلیو. اُنتانگ،ام. و مک دانیال،پی. شناخت امنیت آندروید. مجله امنیت و حریم خصوصی IEEE 7، 1 (ژانویه / فوریه 2009)، 50-57.
9. MODERN OPERATION SYSTEMS (ANDREW S. TANENBAUM )
10. [WWW.GSMARENA.COM](http://WWW.GSMARENA.COM)
11. [WWW.MOBAILESTAN.NET](http://WWW.MOBAILESTAN.NET)
12. [WWW.IR-TCI.ORg](http://WWW.IR-TCI.ORg)
13. [www.AND-ROID.IR](http://www.AND-ROID.IR)
14. [WWW.MICROSOFT.COM](http://WWW.MICROSOFT.COM)
15. [WWW.XDA\_DEVELOPERS.COM](http://WWW.XDA_DEVELOPERS.COM)
16. http://android-developers.blogspot.com/2010/