دراسة أمنية شاملة لنظام الأندرويد

Google Android: A Comprehensive Security Assessment

ترجمة: وائل العلواني

أندرويد 2010
Ardroid.com

هذا البحث يطرح تقييما من الناحية الأمنية لإطار عمل نظام الأندرويد ككل. البحث من إعداد ٦ باحثين من جامعة بن–غوريون العبرية وتم نشره في مجلة IEEE Security & Privacy العريقة في عددها الخاص بشهري مارس/أبريل ٢٠١٠ تحت عنوان

Google Android: A Comprehensive Security Assessment

في هذا البحث، قام الباحثون بتحديد عدد من التهديدات والثغرات عالية الخطورة، وقدموا عددا من الاقتراحات الأمنية التي من شأنها تخفيف هذه المخاطر.

قمنا في أردرويد بترجمة البحث كاملا لإيماننا بأهميته في تعريف قرائنا الأعزاء بالجوانب الأمنية المرتبطة بنظام الأندرويد. وقد حاولنا إضافة بعض الجمل التوضيحية التي من شأنها تقريب المعنى الذي قصده الباحثون وتذليل سوء\صعوبة الفهم الذي قد ينشأ بسبب عملية الترجمة وصعوبة إيجاد المصطلحات العربية التي تؤدي المعنى (وهذا قصور من المترجم وليس ذما بلغتنا العربية الحبيبة :)). ترجمة الدراسة تقع في ١٥ صفحة، وسيتم نشرها على ٣ أجزاء وفي الجزء الأخير سنقوم بإرفاق الدراسة كاملة على شكل ملف PDF.

مقدمة

نظام الأندرويد معرض لهجمات واختراقات أمنية اعتيادية حاله حال أي هاتف ذكي. مثل هذه الهجمات قد يعطل الجهاز جزئيا أو كليا، أو يقوم بإرسال رسائل قصيرة ووسائط متعددة غير مرغوب بها (مما يضيف تكاليف الإرسال الى الفاتورة)، او يكشف معلومات خاصة. وتتضمن مجالات ومنافذ الهجمات: الشبكات الخلوية، بلوتوث، الانترنت (واي فاي و 3G)، منفذ ال USB، وغيرها.

تطور البرمجيات الضارة والفيروسات ومقاومتها لبرامج الحماية سريع جدا بحكم أن مبرمجيها اكتسبوا خبرة عالية من التطور الحاصل في البرمجيات الخبيثة malware المتواجدة في أجهزة الكمبيوتر الشخصية. يقول أحد باحثي أمن المعلومات أليكساندر جوستيف: سنتان هو المقدار الكافي من الزمن لتتطور فيه فيروسات الأجهزة الذكية المحمولة الى مستوى مقارب لدرجة التطور التي وصلتها فيروسات الأجهزة الشخصية خلال ٢٠ سنة. وهذا ما يعني أن التحديات المتعلقة بصد هذه الفيروسات شبيه بتلك الموجودة في الكمبيوترات الشخصية. ولعل أبرز البرمجيات الخبيثة للهواتف الذكية هي من نوع Lasco/Cabir و Commwarrior/Mabir (ديدان ضارة worms) إضافة الى FlexiSpy و RedBrowser و Skulls (أحصنة طروادة) و WinCE.Duts و CardTrap (فيروسات) ومؤخرا دودة iPhone ikee وأداة الاختراق iPhone/Privacy.A التي تستغل العيوب والثغرات التي تنشأ في أنظمة الآيفون المفتوحة jail–broken.

حتى الآن لم تحدث هجمات كارثية تستهدف عددا كبيرا من المستخدمين وذلك لمحدودية عدد الضحايا المكشوفين للهجمات. ولكن ومع الازدياد المتصاعد لعدد مبيعات الأجهزة الذكية (في ٢٠٠٨، مثلت الأجهزة الذكية ١١٪ من نسبة الأجهزة الخلوية المباعة ككل، وهذه النسبة تعدت ال ١٧٪ في ٢٠٠٩) يصبح من المتوقع جدا أن يتم توجيه أنشطة الاختراق بشكل موسع نحو هذه الأجهزة.

المخاطر الأمنية التي تواجه الأندرويد لا يمكن الاستهانة بها، وذلك كونه مفتوح المصدر وهذا ما يتيح للمخترقين دراسة النظام عن كثب وتحديد مواطن الضعف. هذا البحث يشرح ويقيم الآليات الأمنية المتبعة في إطار عمل نظام الأندرويد وتحديد مدى ملاءمتها للتحديات والمخاطر المتزايدة التي تهدد الأجهزة الذكية.

الباب الأول

الآليات الأمنية لنظام الأندرويد Android Security Mechanisms

سنبدأ بتوضيح بعض المعلومات المهمة عن هيكلة نظام الأندرويد وبعدها سنتطرق للآليات الأمنية المتبعة.

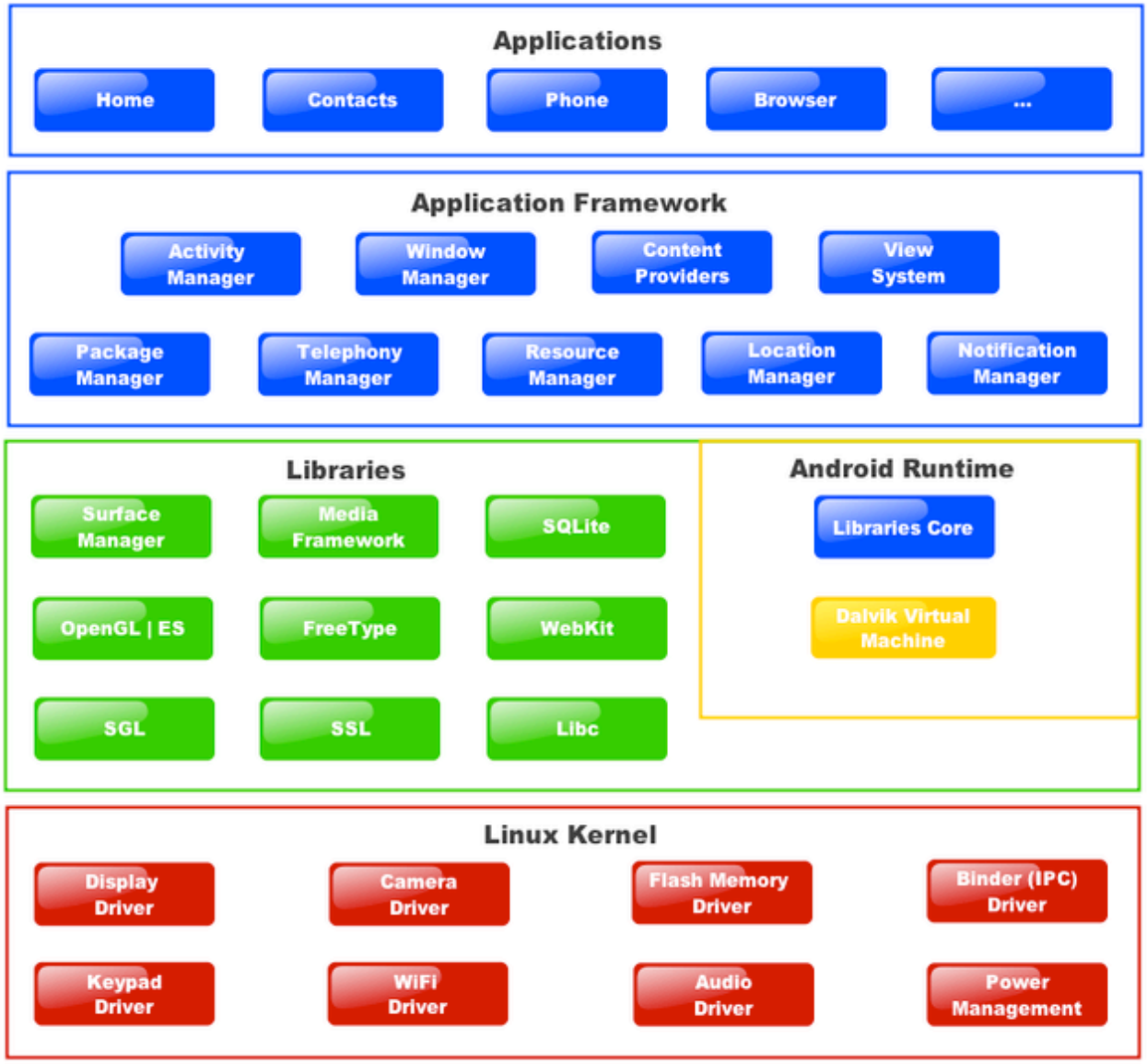
الأندرويد هو بيئة تشغيلية لتطبيقات الأجهزة النقالة. ويتضمن: نظام تشغيل + إطار عمل للتطبيقات + تطبيقات أساسية Core Applications. المكدس البرمجي للأندرويد The Android Software Stack مبني على نواة لينكس والتي تقوم بالتالي:

– التحكم ببرامج تشغيل الأجهزة والملحقات Drivers.

– إدارة الذاكرة Memory management.

– إدارة العمليات Process management.

– إدارة الشبكات وغيرها (انظر الشكل ١).



الشكل ١ (الصورة من موقع ويكيبيديا)

المستوى الذي يعلو نواة اللينكس يحتوي على مكتبات الأندرويد البرمجية الأصيلة Android native library، والتي يتم استخدامها من قبل العناصر الموجودة في المستويات الأعلى. هذه المكتبات مكتوبة بلغة ال C/C++ (تمثل اللون الأخضر في الشكل ١) وهذا يعني تواجد واجهات مكتوبة بالجافا Java interfaces.يأتي فوق هذا المستوى، المستوى التشغيلي Android runtime والذي يحوي آلة افتراضية من نوع دالفيك Dalvik virtual machine والمكتبات الأساسية Core libraries. الآلة الافتراضية Dalvik تشغل ملفات بامتداد .dex وهي مصممة لتكون مدمجة وأكثر فعالية من ناحية الذاكرة المستخدمة مقارنة بملفات مجموعات الجافا العادية Java class files. المكتبات الأساسية مكتوبة بالجافا وتوفر مجموعات جزئية غنية من حزمة Java 5 SE بالإضافة الى بعض المكتبات المخصصة للأندرويد.

المستوى الذي يعلو المستويات السابقة هو مستوى إطار عمل التطبيقات Application framework layer وهو مكتوب بالجافا بالكامل ويحتوي على الأدوات والخدمات المتاحة من غوغل بالإضافة لامتدادات وخدمات أخرى (انظر الشكل ١) .

المستوى العلوي النهائي هو مستوى التطبيقات Application layer والذي يوفر التطبيقات على شاكلة الهاتف، المتصفح، تطبيق الإيميل، . . .

كل تطبيق من تطبيقات الأندرويد يتم تشكيله على هيئة حزمة بامتداد .apk قابلة للتنصيب . هذه الحزمة تشابه الى حد ما حزم الجافا المعروفة jar من ناحية احتوائها على جميع المصادر من كود برمجي الى ملفات الصور والصوت وغيرها الخاصة بالتطبيق . التطبيقات مكتوبة بالجافا باستخدام الحزمة التطويرية البرمجية SDK الخاصة بالأندرويد .

بعد هذه المقدمة التوضيحية، نأتي الى سرد الآليات الأمنية المتبعة في نظام الأندرويد . سيقوم هذا البحث بتقسيم الآليات الى ٣ أقسام : آليات مرتبطة بنظام اللينكس، آليات خصائص البيئة التشغيلية، آليات مختصة بالأندرويد .

أولا : آليات مرتبطة بنظام اللينكس :

هناك آليتان أمنيتان أساسيتان في هذا القسم (على مستوى نواة اللينكس في نظام الأندرويد) : ١– آلية المستخدمين تحت معيار POSIX ٢– آلية دخول الملفات . العنصر الأساسي لهاتين الآليتان هو المستخدم user (ويسمى كيانا) . وكل كائن/غرض Object (كعملية معينة أو ملف) مملوك من قبل كيان\مستخدم (يتم تمثيل المستخدم برقم خاص به، ID) . المستخدمين يمكن تجميعهم وضمهم بمجموعات Groups .

– المستخدمين تحت معيار POSIX : كل حزمة أندرويد .apk منصبة على الجهاز لديها رقم مستخدم فريد unique POSIX user ID . وهذا يعني أن أي حزمتين\تطبيقين مختلفين لا يمكن تشغيلهم في نفس العملية (لا تنس ما ذكرناه في المقطع السابق بأن كل عملية مملوكة من قبل مستخدم واحد) . هذا يخلق نوعا ما صندوقا حول كل تطبيق يمنعه من التداخل مع تطبيق آخر . ولكن مع ذلك، توجد إمكانية تشغيل تطبيقين في عملية واحدة single process بشرط أن يكون كلا التطبيقين يحملان نفس رقم المستخدم user ID وهذا لا يتم الا عبر (١) تفعيل خاصية sharedUserID في ملف المانيفست AndroidManifest.xml الذي تعرضنا له في السلسلة البرمجية التي قمنا بنشرها في أردرويد (٢) توقيع التطبيقين الكترونيا بنفس المفتاح الالكتروني الخاص بالمبرمج (لم نتعرض لهذه النقطة في السلسلة البرمجية التي نشرناها في أردرويد ولكن لتصدير التطبيق على صيغة .apk يتوجب على المبرمج توقيع التطبيق بمفتاح الكتروني digital key خاص به –وبالمناسبة يقوم الاكليبس بهذه المهمة ضمنيا قبل رفع التطبيق على المحاكي، ولكن اذا أراد المبرمج نشر تطبيقه في سوق الأندرويد، فيتوجب عليه القيام بهذه المهمة يدويا وباستخدام مفتاح خاص به مختلف عن ذلك الذي يستعمله الاكليبس–) . وبالإضافة الى كون تفعيل هذه الخاصية يسمح بعمل التطبيقين (أو أكثر) تحت نفس العملية Process، فإنه يمكن للتطبيقين أن يستعملا معلومات بعضهما البعض، أي باستطاعة التطبيق الأول الدخول مباشرة الى معلومات التطبيق الثاني (قاعدة بياناته مثلا) والعكس صحيح .

– دخول الملفات : ملفات النظام والتطبيقات في أندرويد تتبع آليات تصاريح\أذونات لينكس Linux permissions mechanisms . كل ملف مقترن برقم مستخدم يملكه owner user id ورقم المجموعة التي يتبع لها هذا المستخدم، وتصاريح خاصة بالقراءة، الكتابة، والتشغيل Read Write eXecute rwx . وتقوم نواة لينكس بفرض هذه التصاريح بالشكل التالي : التصاريح الخاصة بمالك الملف (٣ قيم)، التصاريح الخاصة بالمستخدمين الذين ينتمون لمجموعة المالك (٣ قيم)، التصاريح الخاصة بباقي المستخدمين (٣ قيم) . مثال : لدينا ملف اسمه whatever.txt، والصلاحيات المعطاة لمالك الملف هي القراءة والكتابة والتنفيذ rwx، وللمستخدمين الذين ينتمون لمجموعة المالك القراءة والتنفيذ فقط rx، ولباقي المستخدمين القراءة والتنفيذ فقط rx، يصبح لدينا التصريح المقترن بهذا الملف : rwxr–xr–x .

مع هذه التصاريح، يتم فرض الجانب الأمني بالشكل المطلوب على المستخدمين عند تعاملهم مع الملفات (التطبيقات وملفات النظام). وبالإضافة لذلك، يتعامل اللينكس مع برامج التشغيل، الصوت، الحساسات sensors، لوحة المفاتيح، وغيرها كما يتعامل مع الملفات، وهذا يعني إضافة التصاريح على إستخدام هذه الوحدات! وهو أمر يعزز جانب الحماية والأمان.

ثانيا : خصائص ومزايا البيئة التشغيلية :

البيئة التشغيلية تعني البيئة التقنية المحيطة كالعتاد hardware، لغة البرمجة، والبنية التحتية لمزود الخدمة ومشغلها. ولهذه البيئة التشغيلية آليات لتعزيز أمن جهاز الأندرويد نبدأ بأولها :

– وحدة إدارة الذاكرة mamory management unit :

من المهم تواجد هذه الوحدة والتي يفترض وجودها العديد من أنظمة التشغيل المعاصرة وعلى رأسها اللينكس. وهي وحدة الكترونية "هاردوير \عتاد" تنظم عملية فصل الفراغات والمساحات المخصصة للعمليات processes في الذاكرة. تستخدمها أنظمة التشغيل للتأكد من أن عملية "س" لا تقرأ ماهو مكتوب في المساحة المخصصة للعملية "ص" في الذاكرة، أو أن تقوم بالكتابة عليها وتعطيلها. هذا من شأنه تقليل احتمالية حصول العملية "س" على صلاحيات أكبر مما تملكه privilege escalation عبر تعديل المعلومات المتعلقة بها في المساحة المخصصة لنظام التشغيل في الذاكرة.

– أمن النوع Type safety :

هذه خاصية من خصائص لغات البرمجة وفيها يتم فرض ضوابط على محتويات المتغيرات variables لتتماهى مع نمط format معين يضمن عدم تحقق أخطاء واستعمال غير مسؤول. الخطر المتأتي من غياب هذه الخاصية يتمثل في حصول عطب في الذاكرة وبالتالي احتمال حصول هجوم buffer_overflow attack وتشغيل كود ضار (وهذا الهجوم يعتبر من أشد أنواع الهجمات خطرا في عالم أمن المعلومات).
تعتبر الجافا أقل عرضة لهذا السيناريو، ولكن التطبيقات والبرامج المكتوبة بلغة سي C (والأندرويد يسمح بتشغيل برامج فيها أكواد مكتوبة بلغة السي) تبقى معرضة لهذا الخطر لأن خاصية type safety غير مفعلة بشكل افتراضي.
في آليات الاتصال بين العمليات Inter_process communication IPC يتم تفعيل هذه الخاصية أيضا للتحقق من أمن نوع البيانات المتبادلة بين العمليات.

– المزايا الأمنية لمزود الخدمة ومشغلها :

تقتبس منصة الأندرويد المزايا الأمنية التي يستخدمها مزودي الخدمة (المصادقة، التفويض، المحاسبة authentication, authorization, accounting) فمثلا المصادقة والتأكد من الأصالة تتم عبر الشريحة SMS.

ثالثا : آليات مختصة بالأندرويد :

يقدم الأندرويد الآليات الثلاث التالية : تصاريح\أذونات التطبيق، تغليف العناصر component encapsulation، التوقيع signing.

– تصاريح\أذونات التطبيق :

يفرض الأندرويد قيودا على التطبيقات التي تسعى للقيام بوظائف معينة ويطلب منها وجود إذن وتصريح. يوجد حوالي ١٠٠ إذن مختلف لتنظيم تنفيذ الوظائف منها على سبيل المثال إذن اجراء اتصال، استعمال الكاميرا، استخدام الانترنت، وحتى إذن توقيف الجهاز عن العمل نهائيا Brick!
يتوجب على التطبيق إذاً توجيه استئذان صريح لتشغيل وظيفة معينة، وهذه التصاريح والأذونات مرتبطة بدرجات حماية :
الدرجة العادية : على مستوى التطبيق نفسه (ليس من الخطر الحصول على إذن لتشغيل عملية ضمن التطبيق نفسه).
الدرجة الخطرة :طلب الحصول على إذن قد يفضي إلى مخاطر معينة كدخول التطبيق إلى بيانات خاصة أو القيام بوظائف معينة، ولذا لا يمكن للتطبيق الحصول على هذا التصريح دون موافقة المستخدم صراحة.

درجة التوقيع: وهو تحصيل أذونات من قبل تطبيقات موقعة بنفس المفتاح الالكتروني لتطبيق آخر تَحَصّل مسبقا على نفس الأذونات من المستخدم.
درجة التوقيع–أو–النظام: حالة خاصة من النقطة السابقة ويتم فيها منح الأذونات بما يشابه النقطة السابقة بالإضافة الى أي حزمة منصبة في ملفات النظام.

إذا أثناء التنصيب، يتم التحقق مما اذا كان التطبيق موقعا بنفس المفتاح لتطبيق سابق (وبالتالي تحقيق الدرجة الثالة أو الرابعة) وإن لم يكن، يتم طلب تصريح المستخدم نفسه (الدرجة الأولى والثانية). وإذا لم يمنح هذه الأذونات أثناء التنصيب، سيفشل في العمل. ولا يمكن لتطبيق أن يطلب مزيدا من التصاريح بعد تنصيبه.

– تغليف العناصر component encapsulation:
يقوم كل تطبيق بإحاطة عناصره وتغليفها في سياقه الخاص مانعا بذلك استخدامها من قبل تطبيقات أخرى (على فرض أن له رقم مستخدم مختلف عن التطبيقات الأخرى POSIX user ID وهو ما ذكرناه سابقا). وهذا يتم بتعطيل خاصية "تصدير exported" العنصر وجعل قيمتها المنطقية "خطأ flase" وطبعا يمكن للمطور تعديلها الى "صواب true" لعناصر معينة يود تصديرها وإتاحتها للتطبيقات الأخرى.

– التوقيع signing:
توقيع التطبيقات وحزم ال .apk كما ذكرت في الأعلى يعتبر صمام حماية حيث أن التطبيق يكون صالحا طالما أن وثيقته الأمنية certificate متوافقة مع المفتاح الالكتروني العام public digital key .

الباب الثاني

التقييم الأمني لإطار عمل الأندرويد

قام معدو البحث بعمل تقييم شامل لعدد من الجوانب الأمنية في أندرويد باستخدام جهاز HTC G1. طرق التقييم تشمل ما يلي:
– مراجعة الكود الخاص بعناصر متعددة في الأندرويد.
– تحليل لآلية منح الأذونات في التطبيقات وعملية تنصيبها.
– تقييم جدوى الأمان والحماية ضد البرمجيات الخبيثة المتوفرة حاليا في لينكس وجافا.

جهاز الأندرويد في حالته العادية محمي بشكل جيد علما أن المهاجم\المخترق لا يمكنه استبدال عناصر النظام الأساسية أو نواة اللينكس دون التلاعب والتدخل المباشر بعتاد الجهاز، وهذا صعب. فإذا السبيل الوحيدة للتلاعب بعناصر نظام التشغيل (سواء النواة أو العناصر الأساسية core componenets) هو بتحديد ثغرة في أحد أجزاء النواة أو العناصر الأساسية ومكتباتها البرمجية تتيح للمخترق الحصول على صلاحيات عالية قد تصل لصلاحيات مستخدم الجذر root. بمجرد تمكن المخترق من استغلال هذه الثغرة فإن بإمكانه تشغيل كود ضار بأعلى درجات الأذونات \الصلاحيات وقد يمكنه هذا الهجوم من التحكم بكل مصادر الجهاز، وذلك لأن العديد من عمليات النظام system processes تعمل تحت صلاحيات مرتفعة (صلاحيات الجذر عادة) ويبقى الأندرويد نظاما مفتوح المصدر، فيمكن للمخترق توجيه ضربات أقوى لعلمه بكيفية عمل النظام برمجيا. بالطبع كون النظام مفتوح المصدر فهذا يكسبه مزايا أمنية عديدة من ناحية تمكين أي شخص عارف بأمور الحماية والأمان تحديد الثغرات المحتملة وتعديلها برمجيا وتعزيز حماية النظام. وهذا يدفعنا لأن نؤمن بأن عدد الثغرات والأخطاء البرمجية آخذ في الاضمحلال الى حد التلاشي نوعا ما مع مرور الزمن. ولكن يبقى احتمال التعرض للهجوم بسبب ثغرات من هذا النوع قائما مهما كان.

مهاجمة جهاز الأندرويد من على بعد تتطلب عمل خدمة service معينة فيها ثغرات أمنية على الانترنت. وهذا السيناريو غير متوقع الحدوث لأنه وبشكل افتراضي، لا تقوم أي خدمة عاملة في النظام بالاستماع لأي اتصال قادم من الانترنت listening for incoming connections. لذا، يمكن اعتبار أن الجهاز معرض فقط لاختراقات على المستوى المحلي host–based عبر الثغرات المحتملة في النواة والخدمات المحلية local services والبرامج التشغيلية وغيرها.

المشاكل الأخرى تكمن في أن آلية منح الأذونات تظل غير محمية بحيث أن سيناريو، على سبيل المثال، منح إذن معين لتطبيق ضار عبر مستخدم غير متنبه للخطورة المتوقعة تبقى قائمة.

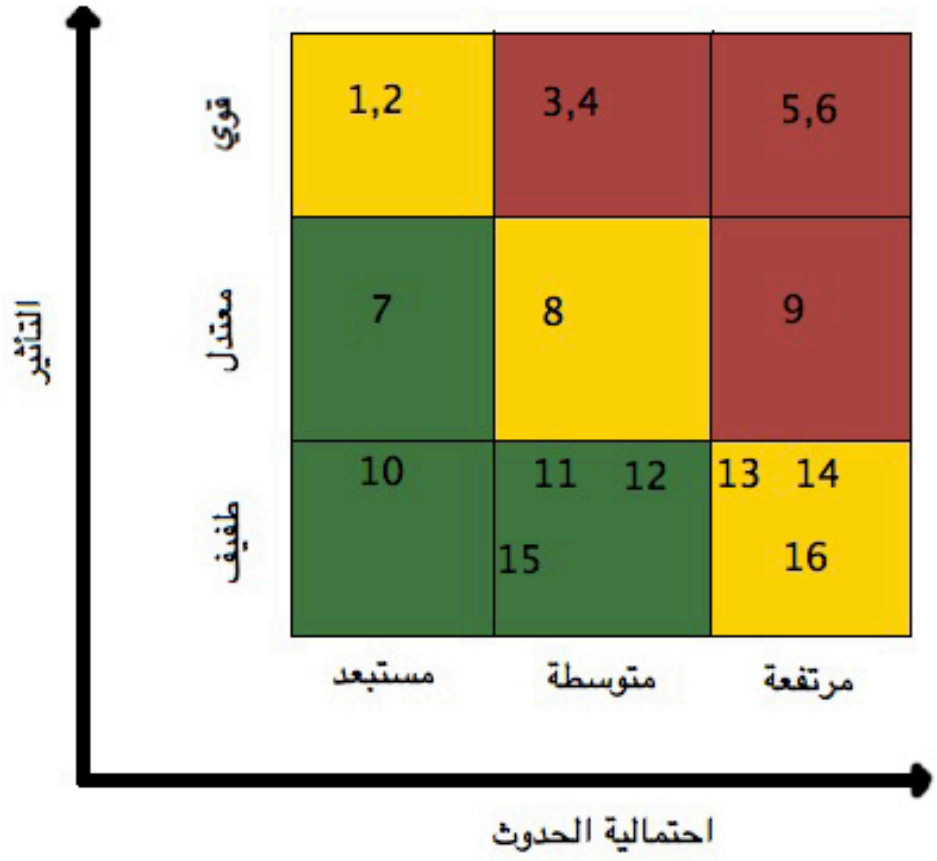
كما أن وجود خاصية رفع التطبيقات على الجهاز بواسطة adb (وهو أمر نستخدمه في الوحدة الطرفية terminal في الكمبيوتر لرفع التطبيقات الى جهاز الأندرويد) وتنصيبها دون أخذ التصريحات والأذونات التي سيستخدمها التطبيق من المستخدم بشكل مباشر تشكل خطرا (وهذا خطر لمسته بنفسي حيث أنك بالفعل تستطيع رفع أي تطبيق ضار الى جهازك الأندرويد عند وصله بالكمبيوتر بسلك اليو اس بي عبر هذا الأمر وسيتم تنصيب التطبيق دون حتى إظهار قائمة الأذونات المطلوبة والتي تظهر عادة عند تحميل وتنصيب تطبيق من سوق الأندرويد).
أضف الى كل ذلك (١) أن الأذونات التي يطلبها التطبيق لا يمكن الموافقة على عدد منها ورفض الباقي، هي أحد أمرين، إما الموافقة على الكل، أو رفض الكل، وهنا تكمن الخطورة في منح الأذونات دون التنبه لأخطار بعضها (٢) التطبيقات التي تشترك في نفس ال user ID أي أن خاصية sharedUserID مفعلة تجعل التطبيقات تتبادل التصاريح والأذونات الممنوحة لإحداها فيما بينها بشكل تلقائي دون إعلام المستخدم.

المشاكل الأخرى التي وجدها الباحثون تتعلق بمتصفح الويب. محرك الويب WebKit المفتوح المصدر والذي يستعمله الأندرويد له تاريخ طويل مع الثغرات التي يتم فيها حقن أكواد ضارة. بعض الهجومات الحالية تتضمن هجوم ال buffer overflow الذي يستغل المكتبات البرمجية الأصيلة القديمة (والتي تكون بحاجة الى تحديث) والهجوم المعروف ب cross_site scripting XSS وهذه الاختراقات تمكن المهاجم من تشغيل أكواد ضارة على الجهاز بالصلاحية الممنوحة لتطبيق تصفح المواقع.

بالنسبة لحقن أكواد وتطبيقات ضارة عبر البلوتوث، فهذا صعب الحدوث لوجود الآليات التالية:
– يمكن وضع الجهاز في طور "غير مرئي not discoverable" عند تشغيل البلوتوث.
– اذا كان في طور "مرئي discoverable" فهذا الوضع يستمر لدقيقتين فقط.
– المستخدم يقوم بالموافقة على انشاء واستقبال اتصال (لا توجد اتصالات دون علمه).
– على المستخدم تنصيب التطبيق أو تشغيل الملف المتلقى يدويا.

بخصوص ما يتعلق بالهجوم المعروف الخاص بحقن جمل ال SQL، أي ال SQL Injection attack، وجد معدوا البحث أن الجهاز محمي منها بشكل جيد. ولكن بنفس الوقت، تبقى بعض المعلومات مكشوفة بالكامل للمهاجم (كمحتويات كرت الذاكرة SD card). ولكن تبقى آلية فرض رقم مستخدم user ID لكل تطبيق بشكل منفصل فعالة في الحماية من التعديل على بيانات التطبيقات والنظام (وهذا ما يحاول هجوم ال SQL عمله عادة).

يوضح الشكل ٢ نتائج تحليل المخاطر النوعية التي قد يتعرض لها الجهاز بالإستناد الى تقييم الأثر الناتج (المحور الصادي العمودي) واحتمالية حصول استغلال لهذه الثغرات (المحور السيني الأفقي) التي من شأنها الحاق الضرر، تعطيل، أو إساءة استخدام الخصوصية أو السرية أو تكامل المعلومات أو طبيعة عمل ما يلي:
– المحتوى الشخصي\الخاص المخزن (صور، ملفات، فيديو، رسائل ايميل، . . .)
– التطبيقات والخدمات (الهاتف، الرسائل القصيرة، الانترنت، . . .)
– موارد الجهاز (طاقة البطارية، هوائي الاتصال وعمله، قدرة المعالج، . .)
– العتاد (الجهاز نفسه، الذاكرة الخارجية\الداخلية، البطارية، الكاميرا، . . .)



الشكل ٢ (مستوحى من الدراسة الأصلية)

شرح الأرقام في الشكل ٢ :

١– اساءة استخدام وظيفة مكلفة (ارسال رسائل قصيرة\وسائط متعددة MMS، اجراء مكالمات هاتفية، تحويل المكالمات الواردة الى رقم ذو تكلفة عالية) باستغلال ثغرة متواجدة في عنصر أساسي في النظام، وهذه الثغرة يمكن الولوج اليها عن بعد عبر الانترنت .

٢– تفعيل نشاط خبيث ضد الشبكة وأجهزتها (ارسال رسائل سبام، الحاق العدوى بالأجهزة الأخرى "بنشر فايروس"، التجسس على حزم المعلومات المتبادلة على الشبكة) باستغلال ثغرة متواجدة في عنصر أساسي في النظام، وهذه الثغرة يمكن الولوج اليها عن بعد عبر الانترنت .

٣– اساءة استخدام وظيفة مكلفة (ارسال رسائل قصيرة\وسائط متعددة MMS، اجراء مكالمات هاتفية، تحويل المكالمات الواردة الى رقم ذو تكلفة عالية) عبر تشغيل تطبيق مضر يستغل ثغرة متواجدة في عنصر أساسي في النظام .

٤– تفعيل نشاط خبيث ضد الشبكة وأجهزتها (ارسال رسائل سبام، الحاق العدوى بالأجهزة الأخرى "بنشر فايروس"، التجسس على حزم المعلومات المتبادلة على الشبكة) عبر تشغيل تطبيق مضر يستغل ثغرة متواجدة في عنصر أساسي في النظام .

٥– اساءة استخدام وظيفة مكلفة (ارسال رسائل قصيرة\وسائط متعددة MMS، اجراء مكالمات هاتفية، تحويل المكالمات الواردة الى رقم ذو تكلفة عالية) عبر استغلال الأذونات الممنوحة أثناء تنصيب تطبيق معين بشكل ضار .

٦– تفعيل نشاط خبيث ضد الشبكة وأجهزتها (ارسال رسائل سبام، الحاق العدوى بالأجهزة الأخرى "بنشر فايروس"، التجسس على حزم المعلومات المتبادلة على الشبكة) عبر استغلال الأذونات الممنوحة أثناء تنصيب تطبيق معين بشكل ضار .

٧– تعطيل الجهاز أو التطبيقات عبر استغلال ثغرة متواجدة في عنصر أساسي في النظام، وهذه الثغرة يمكن الولوج اليها عن بعد عبر الانترنت.

٨– تعطيل الجهاز أو التطبيقات عبر تشغيل تطبيق مضر يستغل ثغرة متواجدة في عنصر أساسي في النظام.

٩– تعطيل الجهاز أو التطبيقات عبر استغلال الأذونات الممنوحة أثناء تنصيب تطبيق معين بشكل ضار.

١٠– تعطيل أو تعديل معلومات ومحتويات خاصة، حجب أو تعديل أو استراق السمع على اتصالات الجهاز مع الشبكة (ارسال رسائل قصيرة، اجراء مكالمات، الانترنت، . . .) عبر استغلال ثغرة متواجدة في عنصر أساسي في النظام، وهذه الثغرة يمكن الولوج اليها عن بعد عبر الانترنت.

١١– تعطيل أو تعديل معلومات ومحتويات خاصة، حجب أو تعديل أو استراق السمع على اتصالات الجهاز مع الشبكة (ارسال رسائل قصيرة، اجراء مكالمات، الانترنت، . . .) عبر تشغيل تطبيق مضر يستغل ثغرة متواجدة في عنصر أساسي في النظام.

١٢– تعطيل أو تعديل معلومات ومحتويات خاصة، حجب أو تعديل أو استراق السمع على اتصالات الجهاز مع الشبكة (ارسال رسائل قصيرة، اجراء مكالمات، الانترنت، . . .) عبر استغلال الأذونات الممنوحة أثناء تنصيب تطبيق معين بشكل ضار.

١٣– التحصل على أو تخريب أو تعديل ملفات ومحتويات خاصة عند تصفح موقع ضار\مشبوه.

١٤– حجب أو تعديل أو استراق السمع (التنصت) على اتصالات الجهاز مع الشبكة في حال اتصال الجهاز بشبكة مشبوهة.

١٥ – استلام رسائل مزعجة (سبام)، رسائل قصيرة ووسائط متعددة SMS/MMS، أو ايميلات.

١٦– ظهور إعلانات في تطبيق متصفح المواقع browser application عند تصفح الانترنت.

١٧– فقد وضياع أجزاء من العتاد.

١٨– إحداث أعطاب في أجزاء العتاد الخاص بالجهاز.

الباب الثالث

حلول أمنية لتحسين أمن وحماية نظام الأندرويد

أفصحت العديد من الشركات عن نواياها لتقديم حلول خاصة بالأندرويد. على سبيل المثال في ٢٠٠٨، طرحت SMobile حلا أمنيا على أجهزة الأندرويد يتضمن برنامجا للحماية من الفيروسات والسرقات. كما قامت شركة Savant Protection المتخصصة في حلول منع التطفل Intrusion Prevention في مارس ٢٠٠٨ بالإعلان عن توفير نسخة من برنامجها Savant Technology على الأندرويد. وشركة Mocana دخلت المجال أيضا بتوفير حل تقني على الأندرويد يملك الميزات التالية: متصفح آمن، عميل آمن للشبكات الافتراضية VPN، حماية من البرمجيات الضارة، تحديث آمن للبرامج وقدرة على إقلاع نظام التشغيل بشكل آمن secure boot، التعامل مع الوثائق الأمنية بشكل آمن digital certificates handling للقيام بعملية مصادقة authenticate الأجهزة، الشبكة، والأفراد. وهناك حل أمني آخر مقدم من DroidHunter.

يفترض الباحثون في هذه الدراسة امكانية تصدير الحلول الأمنية للشركات المعروفة (Symantec, F_Secure, McAfee,...) على منصة الأندرويد ومن أهم المزايا التي ستملكها هذه الحلول في حال تم نشرها خاصيتي الحماية من الفيروسات والكشف عن وجود متطفلين IDS.

يمكن للمستخدمين، بالإضافة للتطبيقات والحلول السابقة، اتخاذ اجراءات إضافية لتعزيز الحماية. وقد قام معدوا الدراسة باختبار عدد منها. فعلى سبيل المثال، قاموا بتصدير خاصية SELinux على الأندرويد والتي تعنى بفرض سياسيات أمنية للتحكم بالدخول Access Control Security Ploicies وذلك بقصد تعزيز حماية عمليات النظام. كما قاموا بتفعيل جدار ناري يعتمد على خاصية NetFilter والتي تتعامل مع حزم البيانات في الشبكة network packets ودراسة كيفية قفل الجهاز وحمايته بكلمات مرور وآليات أخرى. بالإضافة الى كل ذلك، يقوم الباحثون بتطوير واختبار تطبيق يكشف عن وجود الدخلاء والمتطفلين IDS واسمه Andromaly.

الجدول ١ يستعرض الحلول الأمنية القابلة للتطبيق والبرامج والتطبيقات الموجودة لتفعيلها.

الآلية	الوصف	التهديد الأمني	الحلول المتوفرة
مضاد للبرمجيات الخبيثة anti-malware	فحص الملفات، الذاكرة، الرسائل القصيرة، الايميل،..	فيروسات، أحصنة طروادة، root-kits،...	SMobile, Mocana, DroidHunter, CalmAV
الجدار الناري	منع ومراقبة الاتصالات connections غير المسموح بها من والى الجهاز	العمليات المكشوفة لشبكات مشبوهة، هجمات داخل الشبكة	SMobile, NetFilter/ iptables
نظام كشف ومنع المتطفلين IDS	الكشف عن نشاط خبيث أو مشبوه في النظام، العلميات، حزم البيانات على الشبكة، أو في طريقة الاستخدام	نشاط غير معتاد عند اجراء الاتصال، محاولة الوصول لمعلومات خاصة بشكل مشبوه، الهجمات الخبيثة	Andromaly, DroidHunter
التحكم بالدخول Access Control على نظام اللينكس	يتحكم ويحدد عملية دخول العمليات والمستخدمين لموارد الجهاز والنظام	التسبب بعطل بواسطة برمجيات خبيثة وتطبيقات ضارة	SELinux
الدخول Login	يطلب من المستخدم إدخال كلمة مرور لاستخدام الجهاز	استخدام غير مصرح به للجهاز	Android screen-lock pattern وهي الخاصية المعروفة لدينا
أذونات منتقاة Selective Permissions	يخول المستخدم السماح بأذونات منتقاة يطلبها البرنامج أثناء تنصيبه	استخدام أذونات تم منحها بشكل مشبوه من قبل المخترق\المهاجم	

الآلية	الوصف	التهديد الأمني	الحلول المتوفرة
منح الأذونات عبر سياسات معرفة مسبقا	منح الأذونات للتطبيقات أثناء تنصيبها بشكل معرف مسبقا عبر سياسات معينة (يصلح في الأجهزة التي تمنحها الشركات لموظفيها)	استخدام أذونات تم منحها بشكل مشبوه من قبل المخترق\المهاجم	Secure Application INTeraction
تطبيق إدارة الأذونات	فحص الأذونات الممنوحة لجميع التطبيقات وإعطاء المستخدم ملخص عنها	التطبيقات التي لديها أذونات غير مرغوب بها أو مشبوهة، أحصنة طروادة	
تشفير البيانات	تشفير محتويات الجهاز	الدخول الى معلومات حساسة في حال سرق الجهاز أو فقد	
تشفير المكالمات	توفير اتصال آمن (مشفر أو موثوق)	استراق السمع\التنصت، تحديد هوية صاحب الجهاز	
فلترة رسائل السبام	حجب رسائل ال ،MMS SMS، ايميلات، واتصالات من جهات غير مرغوبة	الرسائل المزعجة سبام	
الشبكات الافتراضية الخاصة VPN	الاتصال بشبكة عن بعد عبر الانترنت (ملائمة لموظفي الشركات)	اتصال غير آمن	
شهادات\وثائق الأمان للتطبيقات	توقيع التطبيقات بوثائق ومفاتيح الكترونية موثوقة	التضرر الناشيء من استخدام تطبيقات غير موثوقة	OMTP Application Security Framework
إدارة الموارد	تفعيل التوزيع العادل لموارد الجهاز (المعالج لتطبيقات الجهاز، حصص التخزين في الذاكرة، عمليات الدخول والخروج I/O، استخدام الشبكة	هجمات تعطيل الخدمة DoS	

الآلية	الوصف	التهديد الأمني	الحلول المتوفرة
الإدارة عن بعد	تغيير وإدارة الإعدادات عن بعد (إعدادات الجهاز، إعدادات الجدار الناري، تعطيل الجهاز عن بعد في حال السرقة، تعقب التطبيقات)	سرقة الجهاز	
التحكم بالدخول بشكل تفاعلي ديناميكي	التحكم باستخدام الموارد والخدمات بشكل تفاعلي ديناميكي بناء على قواعد مسبقة	الدخول الى معلومات حساسة أو الإضرار بسير خدمات وعمليات النظام system services	Andromaly, Local app
التحقق من تكامل المعلومات	التحقق من حالة النظام والتطبيقات	العبث بالملفات بشكل يؤثر على عمل التطبيقات والنظام	

الآليات التي ذكرها الباحثون في الجدول ٢ يمكن تقسيمها وتصنيفها في خمس مجموعات\تكتلات، كل مجموعة تمثل خطرا أمنيا واحدا تندرج تحته الآليات المناسبة لحله أو التقليل من أثره وذلك على النحو التالي: (ويتضح مدى فعالية كل آلية واسهامها في تقليل الخطر في المجموعة التي هي جزء منها)

	آليات الحل	درجة الفعالية	الجهد المبذول لتطوير الآلية وتفعيلها
مجموعة التهديدات الأمنية الأولى: استخدام الأذونات الممنوحة لتطبيق تم تنصيبه بشكل ضار وخبيث	نظام كشف ومنع المتطفلين IDS	50%	متوسط
	الجدار الناري	50%	منخفض
	شهادات الأمان للتطبيقات	100%	مرتفع
	أذونات منتقاة	50%	منخفض
مجموعة التهديدات الأمنية الثانية: استغلال ثغرة في نواة اللينكس أو مكتبات النظام البرمجية	التحكم بالدخول Access Control على نظام اللينكس SELinux	75%	منخفض

	آليات الحل	درجة الفعالية	الجهد المبذول لتطوير الآلية وتفعيلها
مجموعة التهديدات الأمنية الثالثة: كشف المحتويات الخاصة\الشخصية	الدخول Login	75%	منخفض
	الجدار الناري	75%	منخفض
	تشفير البيانات	100%	منخفض
	التحكم بالدخول بشكل تفاعلي ديناميكي	75%	متوسط
	الإدارة عن بعد	75%	متوسط
مجموعة التهديدات الأمنية الرابعة: تجفيف\استنزاف الموارد	إدارة الموارد	100%	مرتفع
	نظام كشف ومنع المتطفلين IDS	50%	متوسط
مجموعة التهديدات الأمنية الخامسة: السيطرة والتحكم بالشبكات الداخلية والمحمية التي يتصل بها الجهاز	الشبكات الافتراضية الخاصة VPN	100%	منخفض
	الإدارة عن بعد	100%	متوسط
	التحكم بالدخول بشكل تفاعلي ديناميكي	75%	متوسط

مجموعة التهديدات الأمنية الأولى: استخدام الأذونات الممنوحة لتطبيق تم تنصيبه بشكل ضار وخبيث

هذه المجموعة من التهديدات تستهدف إلحاق الضرر بتوفر الخدمة availability، السرية، وتكامل المعلومات عبر استخدام الأذونات الممنوحة بشكل خبيث. سيناريو الهجوم المقترن بهذه المجموعة محتمل الحدوث وأضراره كبيرة. وتتضمن آليات الحل ما يلي:

١- نظام كشف ومنع المتطفلين IDS:

هذا النظام يعتمد عليه في تحديد السلوك الطبيعي لنظام الأندرويد، التطبيقات، أو المستخدم ويقوم بالكشف عن أي نمط استخدام يشذ عنه، وهذا يكافيء وجود نمط سلوكي لبرنامج خبيث دخيل على النظام. ولكن البرمجيات الخبيثة عادة تتكيف بسرعة وتغير من أنماطها بشكل يجعلها تفلت من نظام ال IDS وهذا ما يقلل من فعالية النظام مع مرور الوقت.

بناء على الجهد الذي بذله معدوا الدراسة في تطوير Andromaly IDS، قاموا بتصنيفه بالمتوسط من ناحية الجهد المبذول لتطويره وبرمجتمه وتفعيله.

٢- الجدار الناري:

يمثل الجدار الناري حلا للهجمات المتعلقة بالشبكات التي يتصل بها الهاتف بحيث يعترض مثلا تسريب المعلومات الذي قد يقوم به برنامج خبيث. كما يمكن لجدار النار الحماية من بعض الهجمات غير المتعلقة بالشبكات.

صنف الباحثون صعوبة تطوير وتفعيل هذه الآلية بالمنخفض وذلك لأن العملية لا تتطلب سوى تفعيل خاصية NetFilter في نواة اللينكس بالإضافة الى عمل تطبيق بسيط يسهل عملية التحكم بهذه الخاصية.

٣- شهادة الأمان للتطبيقات:

هذه الآلية تعتبر مثالية جدا لحل مجموعة التهديدات الأولى. السبب يكمن في أن التطبيقات يتم اختبارها بشكل مكثف وتحديد العواقب الناتجة عن منحها الأذونات التي تطلبها قبل أن يتم توقيعها بالمفتاح والوثيقة الالكترونية التي تضمن خلو التطبيق من أي خطر. اذا، فشل أي تطبيق في الاختبار يعني عدم منحه لشهادة الأمان، وهذا الأمر مطلوب لحل التهديدات الأمنية. ولكن لا شيء يأتي بدون مقابل، فهذه الاختبارات كما هو واضح مكلفة.

٤- أذونات منتقاة:

هذه الآلية تسمح للمستخدم بالموافقة على أذونات محددة من المجموعة التي يطلبها التطبيق عند تنصيبه. تفعيلها يتطلب اجراء تعديل على برنامج تنصيب التطبيقات الموجود في النظام، وقد تم التأكيد مسبقا في هذه الدراسة على أهمية هذه الآلية التي تحمي المستخدم العادي وتقي المستخدم غير الملم بخطورة منح إذن معين لأحد التطبيقات.

تطوير وتطبيق هذه الآلية منخفض عموما و يحتاج الى تعديل طفيف وربما تغييرات سطحية في تصميم النظام.

مجموعة التهديدات الأمنية الثانية: استغلال ثغرة في نواة اللينكس أو مكتبات النظام البرمجية

تستهدف هذه المجموعة استغلال ثغرة في نواة اللينكس أو مكتبات النظام وبالتالي السيطرة والتحكم بتوفر الخدمة، السرية، وتكامل المعلومات (نتيجة مشابهة لما تحدثه المجموعة الأولى). هذا السيناريو تم اثبات احتمالية تحققه من قبل معدي الدراسة كما أثبتت تحليلاتهم وجود ثغرات أمنية إضافية قابلة للانكشاف عبر هذا الهجوم. ولكن تبقى احتمالية التعرض لهذا النوع من الهجوم منخفضة على أنها في حال تحققت فستخلف أثرا مدمرا.

الحل الأساسي هو خاصية SELinux التي تحد من وتتحكم في مقدرات الكيانات المختلفة في نظام التشغيل (مستخدمين، عمليات، . . .) والتي تطال مثلا ما يمكن للعمليات الأساسية وعمليات النظام عمله. إمكانية التحكم بهذا الشكل تضمن عدم إجبار النظام من قبل المهاجم للقيام بعمليات غير مصرح بها. ولكن تبقى هناك أوامر commands اعتيادية لا يمكن ل SELinux منعها والخطر اذا من المدى الذي تعطيه هذه الأوامر العادية للمهاجم وكيفية استغلاله لها لتنفيذ هجومه.

تفعيل SELinux يتطلب جهدا منخفضا بالإضافة الى وضع سياسة\قاعدة policy ملائمة.

مجموعة التهديدات الأمنية الثالثة: كشف المحتويات الخاصة\الشخصية

تهدف هذه التهديدات الى السيطرة والتحكم بتوفر، سرية، وتكامل المعلومات والمحتويات الخاصة. أي تطبيق يمكنه قراءة محتويات كرت الذاكرة SD Card والتنصت على الاتصالات اللاسلكية عن بعد. آليات الحل:

١- الدخول Login:

الآلية المتاحة حاليا سواء لإدخال كلمة مرور أو رسم نمط معين هي آلية فعالة. في حال سرق الجهاز وكانت هذه الآلية مفعلة، فلن يكون هناك خوف مقابل ما اذا كانت هذه الآلية غير مفعلة أو تمت سرقة الجهاز عندما كان غير مقفل. الحل هو أن يتمكن المستخدم من فرض آلية ادخال النمط (تلك التي تظهر عند تشغيلنا للجهاز) على تطبيقات معينة من شأنها الدخول على المعلومات الخاصة.

٢- الجدار الناري:

الجدار الناري من شأنه الحماية من تسرب المعلومات وذلك بمراقبته لحزم البيانات الصادرة والواردة عبر شبكات الاتصال التي تربط الجهاز بجهة أخرى. هذا يمكن الجدار الناري من ايقاف الاتصال في حال الاشتباه بتسريب معلومات خاصة. ما يميز الجدار الناري هو أنه يعمل على مستوى منخفض في هيكل النظام، بمعنى أنه يعمل على مستوى النواة وهذا ما يضمن له تحكما وكفاءة أكبر. وجه القصور في الجدار الناري هو عدم تمكنه من إيقاف الهجوم الذي يقوم بإرسال المعلومات السرية والخاصة عبر رسائل SMS/MMS.

٣- تشفير البيانات :

تعتبر هذه الآلية أفضل حل للحماية من كشف المعلومات الخاصة وذلك لأن المالك هو وحده من يعرف مفتاح فك تشفير البيانات . أي أن البيانات تبقى محمية طالما أن الكلمة السرية\ مفتاح فك التشفير ليس بحوزة السارق وتخمينه يتطلب جهدا ووقتا كبيرين.

أعطيت لهذه الآلية درجة الصعوبة (الجهد المبذول)" منخفض" لأنها بسيطة التطبيق في الأصل كما أنها تتطلب تعاونا من مطوري التطبيقات ليقوموا بحفظ البيانات التي تستخدمها تطبيقاتهم مشفرة. وهذا بدوره يضع مسؤولية أخرى على عاتق غوغل لتحسين النظام في هذا الجانب بجعل التطبيقات الخاصة بال SMS ومعلومات جهات الاتصال Contacts مثلا تحفظ بياناتها مشفرة.

٤- التحكم بالدخول بشكل تفاعلي ديناميكي : Context-Aware Access Control

تتيح هذه الآلية التحكم بالدخول الى المعلومات الخاصة بشكل متغير يعتمد على حالة ووضع الجهاز. من ضمن عوامل السماح بالدخول الى المعلومات : المكان الحالي، الوقت، الشبكة الخلوية، واذا ما كان الجهاز متصلا عبر الواي فاي Wi-Fi وغيرها من العوامل. تخيل لو أن الجهاز سرق وحاول اللص الدخول الى المعلومات الخاصة، ولكن لحسن الحظ، كان المستخدم قد عرف الأماكن الجغرافية التي بالتواجد فيها يمكن دخول البيانات (كالمكتب والبيت)، ففي هذه الحالة لن يتمكن اللص من دخول المعلومات.

الجهد المبذول في هذه الآلية متوسط، فعملية انتقاء القواعد والسياسات policies التي يتم بها التحكم بعملية الدخول ليست بسيطة.

٥- الإدارة عن بعد :

هذه الآلية تكتسب قوتها في حال تم دمجها مع بعض أو كل الآليات التي ذكرت في هذه المجموعة. الهدف من هذه الآلية هو ابقاء التحكم بالجهاز وضبط إعداداته قائما لتقليل الأخطار في حال السرقة مثلا. وهذه العملية مكلفة من ناحية أن التدخل البشري مطلوب بشكل دوري للتأكد من عمل الجهاز، كما أن التدخل في الوقت المناسب لحماية الجهاز عن بعد ضد هجوم معين (يصعب على الانسان القيام بهذا التدخل في الوقت المناسب) يعني وجود تطبيق يقوم بمراقبة الجهاز بشكل مستمر، وهذا مكلف أيضا. ولكن لا شيء يأتي بدون مقابل، لأنه عادة تعزيز الحماية والأمان يقتضي تكلفة أكبر.

مجموعة التهديدات الأمنية الرابعة : تجفيف\ استنزاف الموارد

تستهدف هذه المجموعة من التهديدات اساءة استخدام موارد الجهاز بشكل يؤدي الى استنزافها. بالوضع الطبيعي، لا يتم تخصيص حصص معينة من قدرة المعالج وذاكرة الجهاز RAM للتطبيقات مما يعني أن وجود تطبيق ضار قد يمكنه من استنزاف هذه الموارد. هناك آليتان لحل هذه المجموعة من التهديدات :

١- إدارة الموارد :

توفر هذه الآلية امكانية تلافي الخطر المتأتي من تطبيق ضار يستنزف الموارد. تقوم إدارة الموارد بتخصيص حصص عادلة للتطبيقات بشكل يتناسب مع احتياجاتها وأهميتها (فمثلا تطبيق الهاتف أكثر أهمية من الألعاب). من شأن هذه الآلية الحماية من هجمات DoS في حال كانت قادرة على التحكم بالمخصصات في موارد الجهاز : معالج، ذاكرة RAM، ذاكرة تخزينية، معدل تبادل المعلومات I/O...

يعيبها صعوبة التطبيق وذلك لأنها تتطلب إدخال تعديلات عديدة على النظام.

٢- نظام كشف ومنع المتطفلين IDS :

هذه الآلية تسهم في كشف عمليات استنزاف البطارية أو المعالج عبر ملاحظة الأنشطة غير الطبيعية في استعمال الموارد. في العادة، تتطلع البرمجيات الخبيثة الى عدم إثارة الانتباه، لذلك يتوجب تشغيل ال IDS بشكل مستمر لضبط أي زلة تقع بها هذه البرمجيات.

مجموعة التهديدات الأمنية الخامسة : السيطرة والتحكم بالشبكات الداخلية والمحمية التي يتصل بها الجهاز

يلجأ المخترق عادة الى استخدام جهاز الأندرويد الذي سيطر عليه للسيطرة على أجهزة أخرى، كمبيوترات، وحتى شبكات عبر تشغيل عمليات مسح \ فحص للشبكات ومنافذها أو نشر ديدان عبر الايميل أو SMS / MMS وغيرها. آليات الحلول تتضمن:

١- الشبكات الافتراضية الخاصة VPN :

تعتمد هذه الشبكات على فكرة تشفير الاتصال لحمايته. البروتوكولات التالية: PPTP, L2TP,IPSec والمستخدمة في ال VPN تم تفعيلها على الأندرويد ابتداء من إصدارة 1.6 . تفعيل المزيد من حلول ال VPN يتطلب جهدا منخفضا.

٢- الإدارة عن بعد :

القيام بفرض قواعد وسياسات policies عند الاتصال بشبكات داخلية أو محمية يكون سهلا في حال تم التحكم به بشكل مركزي وذلك بأن يقوم عليه مسؤول شبكات network administrator. ولكن هذه الآلية ذات حدين، فكلما زادت كفاءة المسؤول، يرتفع مستوى تعزيز الأمان والحماية والعكس صحيح.

٣- التحكم بالدخول بشكل تفاعلي ديناميكي :

يتم تفعيل هذه الآلية بالشكل التالي: عندما يتم رصد اتصال بشبكة معينة، تقوم هذه الآلية بفرض عمليات من شأنها ضمان أمن الجهاز. مثلا تقوم بفرض عملية تشفير الاتصال، المصادقة، وغيرها.

الخاتمة

دراستنا التحليلية وضحت بأن الحماية الموجودة على الأندرويد كانت قد صممت بشكل متأن وممتاز لتضمن حماية النظام من العديد من التهديدات والأخطار. وهذا البحث قدم عدد من الآليات والحلول لتعزيز ورفع مستوى الحماية والأمان وقام بتقييمها وتصنيفها.

للإطلاع على معلومات الباحثين الستة الذين أعدوا هذه الدراسة والمصادر التي استعانوا بها:

http://www.computer.org/portal/web/csdl/doi/10.1109/MSP.2010.2