المركز الوطني للمتميزين
The National Center for the Distinguished

Make use of: One ROOT own them all

تقديم : **ألان توما**ت

تاريخ : **2016/2015**

إشراف : **م.علي جنيدي**

ملخص

يقدم هذا البحث أهم المشكلات التي اعترضت وجه مستخدم الـ Android ، وشكّلت عائقاً منعه من التحكم الكامل بنظامه ، فيبحث عن الحل و يبيّن كيفيّة استخدامه ، ويوضح أهمية الـ Root و كيفيّة حلّه لكل المشكلات بإيجابياته و سلبياته .

Make Use Of :

One ROOT Own Them All

Table of Contents

- Introduction……..1

- Part I : ANDROID OS and introducing ROOT……..……2
  - Chapter I : Android OS History and Features……..2
  - Chapter II :Root and Rooting an Android device…….……4

- Part II : Advantages VS Disadvantages and how to do it……..7
  - Chapter I : The Advantages of Root……..…..…..7
  - Chapter II : The Disadvantages of Root……..……12
  - Chapter III : The Solutions……..…..13
  - Chapter IV : Some Root Applications……15
  - Chapter V : How to Root or UnRoot an Android device…20

- Results……22

- Conclusion……23

- Figures' Table……..24

- Sources and References……..25

Abbreviations

OS	Operating System
AOSP	Android Open Source Project
SD Card	Secure Digital
GPS	Global Positioning System
Hz	Hertz
ROM	Read Only Memory
RAM	Random Access Memory
CPU	Central Processing Unit
CWM	ClockWork Mod
APP	Application
WPS	WIFI Protected Setup
WPA	Wireless Protected Access
SU	SuperUser
PIN	Personal Identification Number

Introduction

مع مرور الوقت و التكنولوجيا أصبحت نسبة حاملي الهواتف المحمولة 80% منهم 1.08 Billion أجهزة ذكية فكان دخول Android OS بكل ميزاته خطوة نوعية في مسيرة التطوّر حيث أنّه أصبح النظام الأكثر انتشاراً حول العالم، لكن التطبيقات الجديدة أصبحت تترك المستخدم أمام الحاجة إلى أحدث نسخة نظام على الجهاز القديم مع أن دعم الجهاز قد توقف.

إضافة إلى العدد الكبير من الممنوعات و المحظورات في النظام مما جعل المطورين يرابطون على الحدود غير قادرين على تخطيها حالمين بالسّيطرة التامة.

ممّا أدى لظهور العديد من الفرق التي حاولت حلّ المشكلة و فتح الأفق أمام المستخدم ليصبح SuperUser حاملاً Super Device فكان الحل هو الـ ROOT الذي نشأ ليحل كل هذه الأزمات على يد المطوّرين الّذين استفادوا من كون نواة الأندرويد Linux فطوروا الفكرة حتى أوصلوا الـ ROOT إلى عالم الأندرويد الذي استقبله بفرحة شديدة.

تغيّر الوضع تغيّراً جذرياً و بدأ مستخدمي الـ ROOTيزدادون بسرعة هائلة لمعرفتهم إيجابيّاته و البعض الآخر لم يجرُؤ خوفاً من سلبياته، و تحوّل مجال كتابة التطبيقات و تطويرها إلى تطبيقات تعتمد على الـ ROOT ممّا زاد من فعاليّتها.

فما هو الـ ROOT وكيف ظهر في عالم الأندرويد؟

هل سيتمكّن من حل جميع المشكلات السّابقة؟

الـ ROOT سيف ذو حدّين فما هي إيجابياته وسلبيّاته؟

هل من الممكن الهروب من سلبيّاته و مخاطره على الجهاز؟

لماذا على المستخدم القيام بالـ Rooting؟

كيف حلّ الـ ROOT و تطبيقاته مشاكل الأندرويد و نهض بالجهاز إلى SuperDevice؟

سنجيب عن جميع الأسئلة السّابقة خلال بحثنا هذا.

Part I: ANDROID OS and introducing ROOT

Part I: Chapter I : Android OS History and Features

الشكل (١،١،١)

أندرويد هو نظام تشغيل الهواتف الذكية، وضع بدايةً من قبل شركة أندرويد (Android Inc) و القائمين عليها (أندي روبينAndy Rubin و ريتش مينر Rich Miner ، ونيك سيرز Nick Sears وكريس وايت Chris White) عام ٢٠٠٣ م ثم بيع المشروع لشركة Google عام ٢٠٠٥ م فكانت القائمة على التصميم و التوزيع و التطوير آنذاك ، ثم جعلت من أندرويد مشروعاً مفتوح المصدر (AOSP). [١]

يعتمد Android OS أساساً على نواة لينكس 2.6 تم تطويرها و الإضافة عليها من قبل شركة Google ، فتكون هذه النواة الطبقة الرئيسية التي تقوم عليها كل العمليات و تشكّل أساس النظام.

تعد هذه الطبقة الجزء المسؤول عن تعامل نظام التشغيل مع الجهاز كما أنها مسؤولة عن إدارة العمليات ، إدارة الطاقة ، إدارة الذاكرة بالإضافة إلى إدارة الجهاز (الكاميرا ، الشاشة ...) . [٢]

[1] DHTechnologies / Dominique A.Heger page 1
[2] Rajinder Singh Int. Journal of Engineering Research and Applications page 1

كون نواة النظام Linux هذا أدى لاعتماده نفس مبدأ Linux OS و هو المبدأ المتبّع في كافة أنظمة التشغيل الحاليّة و هو الاعتماد على الملفات أو ما يسمى بنظام الملفات File system ففي الـ Android OS كل شيء موجود ضمن ملف يقوم النظام بقراءته و التعديل عليه فمثلاً عند رفع الصوت يقوم النظام بزيادة الرقم في الملف المسؤول عن مستوى الصوت.

ونتيجة لاتخاذ الـ Android هذا النظام كان على المطورين إيجاد طريقة للحفاظ على الخصوصية و حماية المعلومات فقاموا بالتعديل على النواة لتعمل وفق نظام الصلاحيات أو الأذونات Permissions مما صنف المستخدمين لمستويات و سمح لهم بالتعامل مع الملفات باستخدام العمليات الآتية :

١- القراءة (Read) : السماح للمستخدم بقراءة محتويات الملفات .
٢- الكتابة (Write) : السماح للمستخدم الإضافة و التعديل على الملفات الموجودة .
٣- التنفيذ (Execute) : السماح للمستخدم بتنفيذ الملفات .

سياسة الأذونات المتّبعة حافظت على الأمان أثناء الوصول للملفات ، [1] ولكي يضمن المطورون انتشار النظام كان عليهم تطبيق سياسات تجعل خسارة البيانات و ضرب الخصوصية أمراً مستحيلاً فمنعوا المستخدم من الوصول لملفات النظام الأساسية و التعديل عليها كما يريد ، مما زاد من الخصوصية و إمكانية الحفاظ على البيانات ، لكن هذا شكل حاجزاً في وجه المبرمجين الهواة و المحترفين الذين أرادوا الحصول على التحكم الكامل بالنظام فأنشؤوا ما سُميّ بالـ Root و معناه الجذر للدلالة على الوصول إلى جذر النظام .

[1] Rajinder Singh Int. Journal of Engineering Research and Applications page 2

الشكل (٢،١،١)

Part I : Chapter II :Root and Rooting an Android device

Rooting Process :

- هي العمليّة التي يمكن للمستخدم من خلالها تعديل نظامه ، و الحصول على تحكم عال المستوى بالنظام و أساساته ، بالتالي تجاوز كل الحدود الموضوعة من قبل المطوّر .[١]
- أتى مصطلح الـ Root من نظام الملفات و الأذونات في أنظمة التشغيل UNIX , LINUX فيكون جذر نظام الملفات هو بداية كل الملفات ، و جذر نظام الأذونات هو بداية كل الأذونات بالتالي أقوى الامتيازات. حيث أن مستوى الـ Root موجود لتوفير الوصول الإداري Administrative Access للنظام مما يتيح إمكانية القراءة و التعديل على كافة ملفات النظام و تغيير إعداداته ، لذلك فإن الهدف الأسمى لل Hackers هو تسجيل الدخول على جهاز LINUX بمستوى Root .[٢]

[1] Take Control : Android Rooting Guide / Alexander Cordova / page 4
[2] XdaDevelopers' / Android Hacker's Toolkit / Jason Tylor & Will Verduzco / page 27

الشكل (١،٢،١)

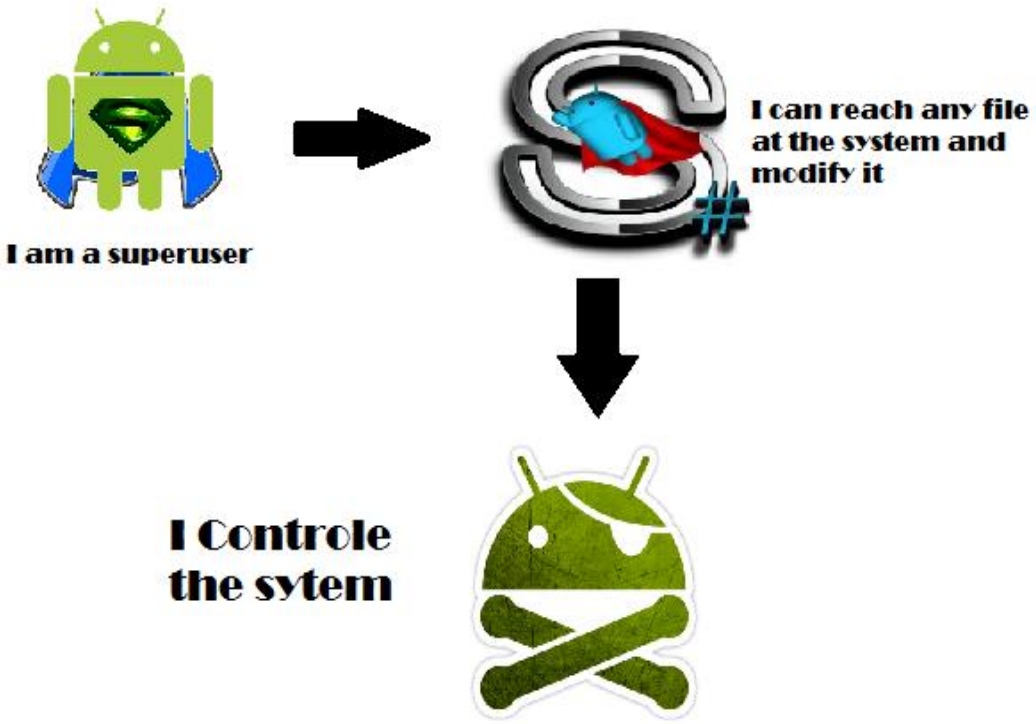
الشكل(١،٢،٢)

- نشأت عن أنظمة ال Unix , Linux عندما دعت الحاجة لحماية الخصوصية الفردية للمستخدمين و تشغيل النظام بميزاته ، فتوجب إيجاد حساب مميّز عن الحسابات الأخرى يمكّن مالكه من التحكم بأساسيات النظام و له الصلاحيات الكاملة SuperUser Account (مثيل Administrator Account في Windows)على عكس الحسابات البقية التي لها صلاحيات أقل User Accounts . [1]

بالتالي يمكن استنتاج تعريف Rooting مما سبق :

الـ Rooting : هي عملية الحصول على حساب Administrator أو حساب SuperUser يتيح للمستخدم تجاوز كل الحواجز التي وُضعت من قبل المطوّر فتعطيه كامل الصلاحيات للقيام بالقراءة و التعديل على ملفات النظام وبما أن النظام يعتمد أساساً على نظام الملفّات بالتالي أصبح لـ SuperUser إمكانية التحكم بالنظام .

[1] Learning Android Forensics / Rohit Tamma & Donnie Tindall / page **59**


I am a superuser
I can reach any file at the system and modify it
I Controle the sytem

الشكل(١،٢،٣)

Part II : Advantages VS Disadvantages and how to do it

في هذا الفصل سنتحدث عن اتخاذ قرار شبه مصيري بالنسبة لمستخدمي الأندرويد ، هل هم حقاً بحاجة لذلك ؟

كل شيء ذو حدين لكن أثبتت الدراسات أن معظم مستخدمي الـ Root للمرة الأولى لم يستطيعوا العودة لحياتهم العادية بعد فتح الآفاق أمامهم . فإن فوائد القيام بتلك العملية كثيرة جداً منها : توفير المال و تحديد المشاكل التي تنشأ أثناء التطوير و إزالة القيود المفروضة من قبل المصنّع ، بالإضافة للنهوض باستخدام الجهاز إلى أعلى المسويات ، لكن هذه الخدمات تفرض مخاطر كثيرة.

Part II : Chapter I : The Advantages of Root

الشكل (٢،١،١)

❖ **زيادة فترة خدمة الجهاز (Increasing The Service Life of The Device) :**

منذ إطلاق أول جهاز أندرويد HTC Dream بدأ الإقبال على أجهزة الأندرويد و بدأت تنتشر أكثر و أكثر فازدادت سرعة التطوير و ازداد عدد أجهزة الأندرويد و اختلفت قدراتها ، فلجأ المنتجون

للتخلي عن دعم الأجهزة القديمة و إزالة العوائق منها و توجهوا لإنتاج الأحدث ، لكن ما الذي حل بمستخدمي الأجهزة القديمة ؟

عندما لاحظ المبرمجون العدد الكبير من مقتني الأجهزة القديمة ، بدؤوا ضمن فرق منعزلة بتطوير أنظمة أندرويد لتلائم جميع الأجهزة. لكن لكي يستطيع المستخدمون تحديث أنظمتهم كان عليهم أن يصلوا لجذر النظام لديهم و أن يتخطوا قيود المنتجين التي أوقفت التحديثات عند نسخة أندرويد محددة فكان الحل الوحيد الـ Root ؛ بهذا تمكن الـ Root من إطالة مدة استخدام الجهاز عن طريق إتاحة إمكانية التحديث لآخر نسخ الأندرويد.

❖ تصحيح أخطاء المصنعين :

كنتيجة للسرعة الكبيرة في إنتاج الأجهزة Hardware لمواكبة سرعة تطور الأندرويد كـ Software بدأت العيوب تظهر في التصاميم و بعض هذه العيوب كان صغيراً كتعامل بطيء جداً مع SD Cards ، أما بعض الأجهزة قد تم إنتاجه وبيعه مع أخطاء فادحة في العمل كـ Samsung Galaxy S الجهاز المشهور حول العالم ؛ حيث أن الاهتمام بالشكل الخارجي و الانثناءات تحديداً أدت لتوضع خاطئ لمستقبل الـ GPS بالتالي تحديد مواقع خاطئة .

صحيح أنه من الصعب حلّ مشاكل الـ Hardware باستخدام الـ Software لكن المجتمعات البرمجية تمكّنت من حل معظم المشاكل عن طريق التعديل في موضوعات المصنّع ، وحتى يتمكن المبرمجين من ذلك علهم الحصول على إذن وصول و تعديل و هذا ما أتاحه الـ Root لهم .

❖ زيادة القدرة (Increasing Capability) :

تقريباً كل جهاز أندرويد يحمل وحدة معالجة مركزية تستطيع العمل بقدرة أكبر بكثير ممّا وُضِعت عليه من قبل المصنّعين و ذلك بهدف إطالة عمر البطارية قدر المستطاع و تجنّب قضايا ارتفاع حرارة الجهاز .

مثلاً جهاز Xoom (Motorola Android tablet) يعمل معالجه بتردد GHz 1 مع أنه قادر على العمل بتردد قد يصل إلى 1.4 أو GHz 1.5 بشكل آمن مما يعطيه أداء فائق الروعة .

فكل أجهزة الأندرويد قابلة لزيادة تردد المعالج CPU لتعطي أداءً عالياً و تسمى هذه العملية Overclocking (رفع تردد التشغيل) ، لكن حتى نستطيع ذلك يجب أن نُعطى إذناً بالوصول و التعديل و هذا ما يوفره الRoot .

Overclocking

هو مصطلح يعني " إعطاء سرعة أكبر " و يأتي من الفكرة التقنية التي تقوم عليها سرعة المعالج في الحاسوب "Clock Cycle" مقاسة بالهرتز Hz . فسرعة 500 MHz أو 1 GHz تعني عدد الـ Clock Cycles التي تمر في المعالج في الميللي ثانية .

فالـ Overclocking هو تشغيل المعالج بسرعة أكبر من سرعتها الأصلية و هذا عادةً يعني زيادة الفولطية المقدّمة مما يعني استهلاك أكبر للبطارية ، زيادة حرارة المعالج و زيادة سرعة و أداء الجهاز

XdaDevelopers' / Android Hacker's Toolkit / Jason Tylor & Will Verduzco / page 30

❖ **تخصيص الجهاز (Customizing the device) :**

مع أنه ليس سبباً قوياً إلّا أن رغبة المطورين بالحصول على التحكم الكامل بالمظهر في أجهزتهم يدفعهم للقيام بالـ Root ، ففي الحالة الطبيعية يملك المستخدم قدرة محدودة جدّاً في التعديل على بعض أجزاء نظام الملفات ، أمّا الـ Root فيعطيهم القدرة الكاملة على التعديل حتى في الأجزاء الغير قابلة لذلك .

لقد انصبّ اهتمام المطورين بشكل ملحوظ على إنتاج Custom Recoveries و Custom ROMs مع أن العملية تستغرق وقتاً طويلاً ، مما أتاح للمستخدم قدرة كبيرة بتحويل جهازه إلا الجهاز الذي كان يحلم به . فلولا الـ Root لما استطاع المطورون كتابها و تطويرها.

Recovery mode

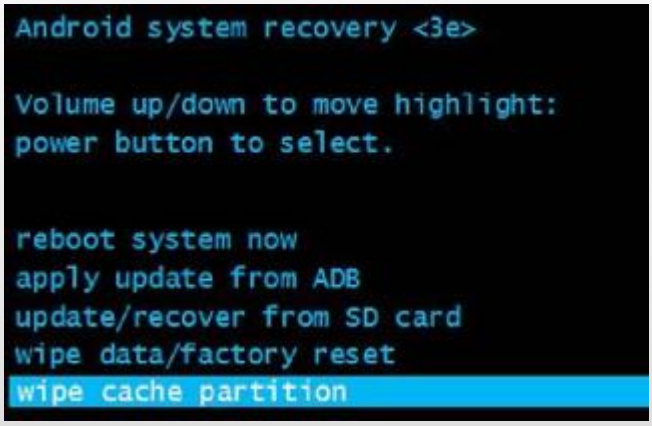
يمكن النظر إلى جهاز الأندرويد على أنه جهاز يحمل ثلاثة أجزاء رئيسية هي :

١- Boot Loader : هو القسم الأول من الجهاز و هو أول برنامج (برمجية) تمر على المعالج عند تشغيل الجهاز وظيفته تكمن في الاهتمام بتهيئة العتاد الصلب و إجراء فحص له بالإضافة إلى إعداد إقلاع الجهاز Boot و تسليم العمل للبرمجية التي تليه و عي غالباً الـ Android ROM .

٢- Android ROM : يحمل جميع الملفات اللازمة لبدء تشغيل النظام .

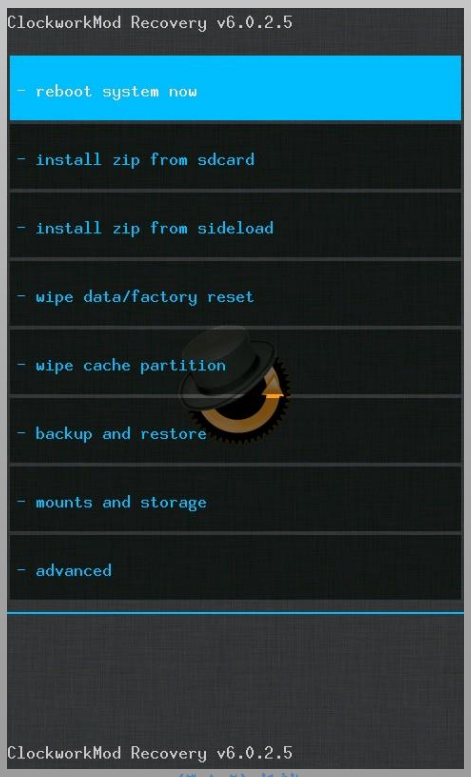
٣- Recovery : هو عبارة عن وضع يمكن الانتقال إليه قبل استلام Android ROM زمام الأمور و هي نوعان :

- Stock Recovery : هي الـ Recovery الموجودة على الجهاز من الأصل تتألف من واجهة بسيطة جداً للتعامل مع المستخدم و يتم التعامل معها عن طريق أزرار الـ Hardware و تكون وظيفتها محدودة جداً تقتصر على : إعادة زمام الأمور للنظام ، تثبيت التحديثات من بطاقة الذاكرة ، إعادة ضبط بيانات المصنع .
نحن نعلم أنه يمكن القيام بذلك من النظام لكن في الواقع النظام يقوم تلقائياً بإعادة تشغيل الجهاز و التحويل إلى وضع الـ Recovery ثم القيام بالتحديث أو إعادة ضبط المصنع .

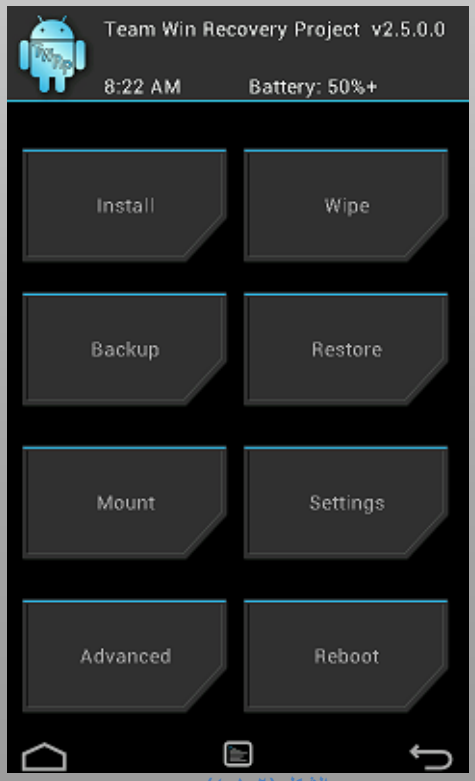


الشكل (٢،١،٢)

- Custom Recovery : توفر ميزات أكثر من الـ Stock recovery حيث تضمن :
  - حفظ نسخة احتياطية كاملة من النظام Full Backup .
  - السماح بالتحديثات غير الرسمية أو بالرسمية مع مفاتيح مخصصة .
  - التعامل مع الـ Recovery لمساً .
  - أشهر الـ Custom Recoveries : هما CWM Recovery (ClockWorkMod Recovery) و Team Win Recovery .[١]



الشكل (٣،١،٢)



الشكل (٤،١،٢)

❖ **حفظ نسخة احتياطية من البيانات (Backing up Data) :**

الـ Root يسهّل أخذ نسخة احتياطية من المعلومات الموجودة على الجهاز كما أنه يوفّر أخذ نسخة احتياطية من النظام بأكمله و بكامل التطبيقات المتوفرة عليه خصوصاً بوجود Custom Recovery .

التطبيقات و بياناتها (Applications and its Data) :

عند تحميل التطبيقات من أي متجر كـ Google Play و انقطاع الاتصال بالشابكة، فإنه عند إعادة الاتصال يتم استئناف التحميل من نقطة الانقطاع و ذلك لأن معلومات الحساب التي تم الاتصال عن طريقها بالإضافة لكافة المعلومات الخاصة بالتطبيقات قد تم تخزينها على مخدّمات Google.

كما هو الحال في أجهزة الأندرويد فإنه لمنُ المعلوم إمكانية نقل الصور والموسيقى إلى بطاقة الذاكرة SD Card.

كما أنه يمكننا نقل التطبيقات من Application manager على أجهزتنا إلى بطاقة الذاكرة أيضاً، لكن ماذا عن معلومات هذه التطبيقات (المعلومات التي يتم تخزينها على الجهاز نتيجة تعامل المستخدم مع التطبيق) ؟؟؟

هذه المعلومات تُخزن على الجهاز في مجلّد الـ Data الخاص بنظام الأندرويد ولا يمكن للمستخدم العادي نقلها إلى بطاقة الذاكرة لأن المصنّعين لم يزوّدونا بهذه الإمكانية لكن الـ Root قد فعل.

يتيح الـ Root نقل معلومات كافة التطبيقات إلى بطاقة الذاكرة كما يتيح تشغيلها انطلاقاً من البطاقة SD Card.[1]

الشكل (٢،١،٥)

[1] XdaDevelopers' / Android Hacker's Toolkit / Jason Tylor & Will Verduzco / page 27 , 28 , 29 , 30 , 31

Part II : Chapter II : The Disadvantages of Root

الشكل(٢،٢،١)

مخاطر الـ Root كثيرة ولكن لحسن الحظ واضحة ومعروفة كما أن احتمال الوقوع فيها قليلة جداً.

١- أول المخاطر وأسوؤها على الإطلاق (bricking the device) وكلمة Bricking قد تعني حصول أمرين:

- توقف الجهاز عن العمل نهائياً.
- دخول الجهاز بحالة تسمى BootLoop أي تكرار إقلاع الجهاز إلى ما لا نهاية.

٢- مع القوة الهائلة تأتي المسؤولية الكبيرة فصحيح أن عملية الـ Rooting تعطي المستخدم قوة الـ SuperUser إلّا أن الـ Root يخترق جدار الحماية الذي وُضِع من قبل المصنّع و يترك ثغرات فيه تسمح للمستخدم بتثبيت تطبيقات غير معترف بها من قبل سوق تطبيقات الأندرويد؛ فالتطبيقات الخبيثة واقع مؤلم في سوق الأندرويد، و يتراوح ضررها من صغير إلى كبير جداً لإضافة لاختراق الخصوصية نتيجة الثغرات التي تركها الـ Root في جدار الحماية .

٣- الخطر الثالث و الأخير: هذه المشكلة لا يمكن الهروب منها أبداً و هي فقدان الضمان المقدّم من الشركة ، حيث تصبح الشركة غير مسؤولة عن أي عطل أو عطب يصيب الجهاز و قد

صرّحت عن ذلك كافة شركات الأجهزة ، و يرافق سحب الضمان منع التحديثات الرسمية التي كانت متاحة للجهاز .[1]

أعتقد أن هذه المخاطر غير محبّذة لدى جميع مستخدمي الأندرويد المترددين بالنسبة للحصول على الـ Root وقد تجعلهم يلغون الفكرة تماماً؛ لكن ماذا لو وضعنا حلّاً لكلّ مشكلة من المشاكل السابقة.

Part II: Chapter III: The Solutions

المشكلة الأولى و الأخطر يمكن تجنّبها ببساطة شديدة و ذلك بعدم القيام بالـ Root إن لم يقم به قبلك أحد يملك نفس جهازك، ذلك لأن هذه المشكلة تظهر بالنسبة لنوع الجهاز، فجميع الشركات تعمل على زيادة الأمان عن طريق تشفير كل العمليّات التي تحدث في الجهاز، فهذا أحياناً يؤدي لتوقف الجهاز عن العمل نهائيّاً لكن سرعان ما يجد المطورون طريقة أخرى للقيام بالـ Root على هذا النوع .

أمّا المشكلة الثانية فتكمن في التطبيقات الخبيثة التي من الممكن أن تضر الجهاز، فلنفترض أنني SuperUser فمن أين أحصل على تطبيقات الـ Root خاصتي؟

الجواب بسيط للغاية فأول مكان هو Google Play فلم يتم منع تطبيقات الـ Root عنه على الأقل ليس أغلبها، و من المعلوم أن تطبيقات Google Play آمنة لأنها مجرّبة من قبل شركة Google .

لكن هنا تجدر الملاحظة أن معظم تطبيقات الـ Root الموجودة على Google Play غير مجانية أو أنهم يقدمون فترة مجانية ثم يجب على المستخدم الدفع للحصول على نسخة كاملة فما الحل؟

الحل هنا يتّبع الحالة فإن كان التطبيق غير مجاني أو غير موجود في المتجر فهو حتماً موجود لدا فريق XDA Developers بالإضافة إلى أنه مجاني و يمكن التحميل من موقعهم الرسمي http://forum.xda-developers.com .

أما إن تمّ إعطاؤك مهلة مجانية فالأمور تصبح أسهل أكثر فأكثر؛ حيث أن تطبيق Lucky Patcher يوفر لمستخدمي الـ Root رفع قيود متجر Google Play ويحوّل النّسخة التجريبيّة إلى كاملة. بهذا تكون المشكلة الثانية قد حلّت.

[1] Take Control : Android Rooting Guide / Alexander Cordova / page 15

المشكلة الثالثة والأخيرة (فقدان الضمان): لقد قلنا سابقاً أنه لا يمكن الهروب من هذه المشكلة لأنه حالما تقوم بالـ Root لجهازك ستعلم الشركة بذلك تسحب الضمان، بكن كيف تعرف الشركة بذلك؟

Flash Counter

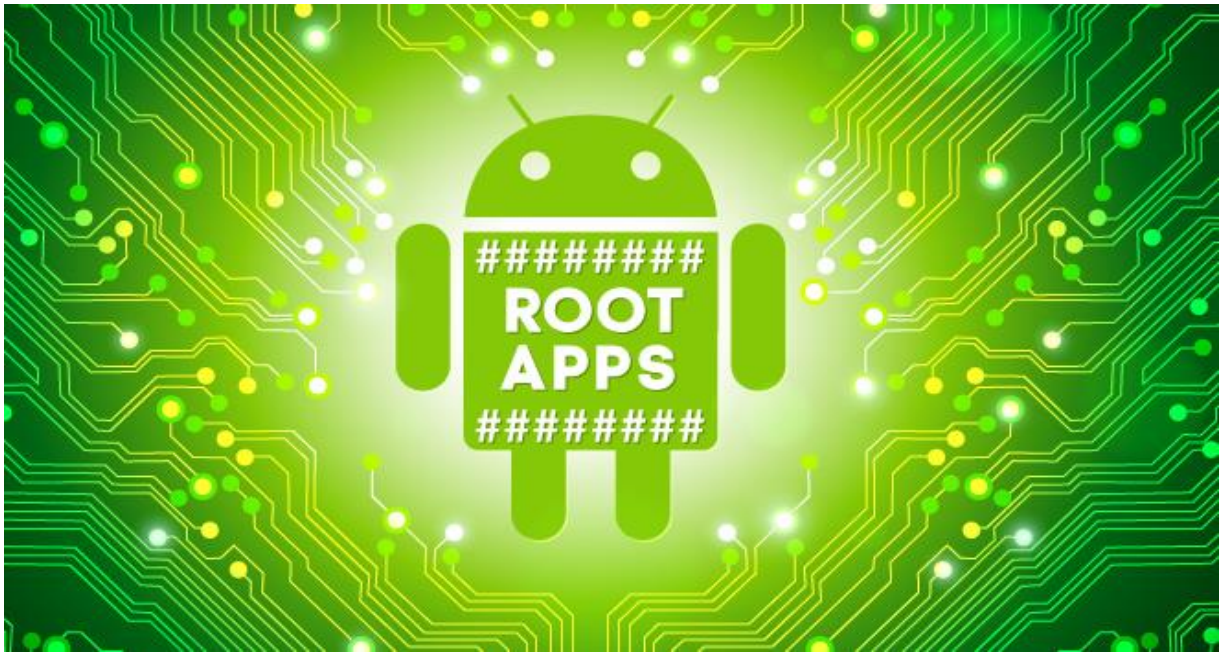
تحتوي أجهزة السامسونج ما يسمى عدّاد تفليش Flash Counter تكون قيمته الافتراضية 0 و تقوم بالزيادة بمقدار 1 لكل تعديل جذري في الجهاز كتغيير Android ROM إلى نسخة غير رسمية أو تثبيت Custom Recovery أو القيام بالـ Root للجهاز و هو محمول على وضع يسمى Download Mode الذي يعد الطبقة الأساس التي تحمل كل شيء فعن طريقه يمكن تغيير الـ Recovery mode.

http://forum.xda-developers.com/galaxy-s2/orig-development/2014-01-15-triangleaway-v3-

بالتالي كل ما أحتاج إليه لإعادة الضمان هو جعل العداد صفراً، و يتم هذا عن طريق برنامج طورّه XDA Developers يمكنه إعادته للصفر Triangle away يمكن تحميله من موقع الفريق الرسمي أو من Google Play.

لكن هنا تجدر الملاحظة أولاً أن البرنامج يحتاج Root لذا بعد تصفير العداد لا مشكلة بالاحتفاظ بالـ Root ، لكن بوجود ROM معدّلة سيعود العداد إلى الواحد مجرّد إقلاع الجهاز لذلك يجب الحصول على ROM رسمية للتمتع بالضمان كاملاً و هذه ليست بمشكلة لأن معظم المستخدمين يحتفظون بنسخة احتياطية لل ROM الأصلية قبل تغييرها ، بهذا نكون قد حللنا المشاكل الثلاث.

Part II : Chapter IV : Some Root Applications .



الشكل(٢،٤،١)

سنتحدث في هذا الفصل عن بعض تطبيقات الـ Root ووظيفة كلّ منها .

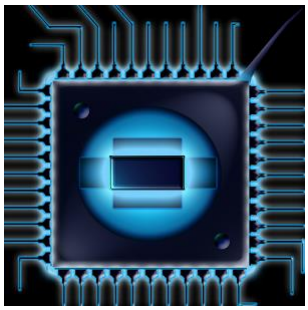
1- SET CPU :

الشكل(٢،٤،٢)

تحدثنا سابقاً عن أن الـ Root يتيح عملية الـ Overclocking ، و هذا التطبيق يتيح التحكم بهذه الميزة عن طريق وضع الحد الأدنى لقدرة المعالج و الحد الأعلى و من ثمّ تحديد خطة العمل كأن تكون الخطة تفاعليّة فيتغيّر تردّد المعالج ضمن المجال الموضوع حسب حاجة الجهاز مما يقلل من العبء على البطارية ، أو أن تكون الخطة أداءً عالياً فيبقى التردد ثابتاً على الحد الأعلى المحدّد من قبل المستخدم.

تجدر هنا الملاحظة أن بعض الـ ROMs المخصصة تتيح التحكم بالمعالج تلقائياً دون هذا البرنامج و ذلك لأن الـ Root موجود أصلاً مع هذه الـ ROMs و أشهرها CyanogenMod .

2- RAM Manager Pro :



الشكل(٢،٤،٣)

مهمّة هذا التطبيق تحسين أداء الذاكرة العشوائية RAM عن طريق تنظيفها أو ضبط خطة لعملها فهو يتيح الخطط التالية :

More free Memory , More Multitasking , Hard Gaming , Hard Multitasking

بالإضافة لأنه يتيح للمستخدم إنشاء الخطة الخاصّة به ، كما أنه يقوم بإظهار مدى استهلاك الـ RAM و ما الّذي يستهلكها .

3- Game Killer :

الشكل(٢،٤،٤)

يستطيع التطبيق بأمر من الـ Root الوصول لملفات الـ Data الخاصة بجميع التطبيقات و التعديل عليها.

إن أراد المستخدم تغيير رقم ما في تطبيق كرصيد المال في لعبة فما عليه إلّا أن يبحث عن الرقم الحالي ثم تغييره و البحث عن الرقم الجديد ليتم البحث ضمن النتائج و هكذا حتى الوصول إلى القيمة المطلوبة و تغييرها.

مثيله على الحاسوب Cheat Engine.

4- WIFI Kill :

الشكل(٢،٤،٥)

يستطيع هذا التطبيق الوصول إلى جميع المتصلين بالشبكة التي يكون الجهاز متصلاً بها و إحضار عناوين الـ IP الخاصّة بهم مع إمكانية قطع الشبكة عنهم.

مثيله على الحاسوب Net Cut.

5- GL to SD Card :

الشكل(٢،٤،٦)

تحدثنا سابقاً عن التطبيقات و بياناتها و هذا التطبيق مسؤول عن نقل بيانات التطبيقات إلى بطاقة الذاكرة و تشغيلها عن البطاقة .

6- Disk Digger :

الشكل(٢،٤،٧)

هذا التطبيق مسؤول عن استعادة الملفات المحذوفة عن جهاز الأندرويد لكن كلما أسرع المستخدم باستعادتها كانت النتيجة أضمن لأن التطبيق لا يتعامل مع ملفات بل مع خانات ذاكرة فإذا كُتب فوق خانة ما لا يمكن استعادة ما كان قبلها لذلك يُنصح بعدم تحميل أي شيء على الجهاز قبل الاستعادة.

مثيله على الحاسوب Recover my Data.

7- zANTI :

الشكل(٢،٤،٨)

يصل هذا التطبيق للأجهزة المتّصلة بنفس الشبكة و يحدد الثغرات الموجودة في كل جهاز فيحوّله إلى فريسة و يتيح الكثير : كتبديل جميع الصور الموجودة على الويب و الظاهرة للمستخدم بصورة يحددها المخترق كما يستطيع نقله إلى صفحة ويب يحدده المخترق أيضاً أو إيقاف التحميل عند الفريسة و لكن الشرط الوحيد أن تكون الفريسة ضمن بروتوكول http و ليس https المشفّر .

8- Triangle away :

الشكل(٢،٤،٩)

تحدثنا سابقاً عن هذا التطبيق ووظيفته جعل عدّاد التفليش Flash Counter صفراً و إعادة الضمان في أجهزة SAMSUNG.

9- Wps Wpa Tester :

الشكل(٢،٤،١٠)

هذا البرنامج يجسّد معنى اختراق الشبكات في الأندرويد و هو يستخدم الثغرة الموجود في الـ WPS .

مثيله على الحاسوب Dumper .

WPS (WIFI Protected Setup)

WPS هو عبارة عن وسيلة تم تطويرها وتقديمها من قبل اتحاد Wi-Fi لمساعدة المستخدمين على إعداد اتصالاتهم اللاسلكية بأجهزتهم فباستخدامها تتمكن بالضغط على زر فقط فيتم الاتّصال تلقائيّاً عند تفعيل الخاصية ذاتها على الجهاز المتصل.

يتم ذلك بإحضار رقم PIN الخاص بالـ Router و الاتصال عن طريقه .

قام Stefan Viehböck بالتبليغ عن خطأ في تصميم WPS يؤدي إلى تخفيض الزمن اللازم للهجوم بغية كشف PIN و الحصول عليه .

هذه الثغرة موجودة في أنواع الـ Router التالية :

D-Link, Linksys, Netgear, TP-Link, ZyXEL, Belkin, Buffalo, Technicolor .

Part II : Chapter V : How to Root or UnRoot an Android device.

Rooting :

كانت عمليّة الـ Rooting في البداية صعبة و تتعلق بنوع الجهاز، فلكل جهاز طريقته حتى أصدر المطورون البرنامج الأشهر Kingo Root الذي ضم أكبر عدد من الأجهزة المدعومة فأصدروه بصيغة apk. و جعلوا العمليّة كلها تحتاج لضغطة واحدة . يمكن تحميل التطبيق من الموقع الرسمي.

http://root-apk.kingoapp.com

كما قام مبرمجو XDA بتطوير برنامج آخر يدعى FramaRoot حيث يدعم العمليتين Rooting UnRooting, و يعمل على عدد كبير جداً من الأجهزة و هي مبيّنة في الرابط :

http://forum.xda-developers.com/apps/framaroot/framaroot-supported-devices-t2722980

هنا يجب الإشارة إلى وجود عدد كبير من الرومات المعدّلة التي تحوي Root Access بطبيعتها كأية ROM من Cyanogenmod.

UnRooting:

من الممكن إزالة الـ Root من جهاز الأندرويد بطرائق عدة إن لم يكن من أصل الـ ROM.

من خلال تطبيق SuperSU يمكن إزالة الـ Root بالكامل من أي جهاز أندرويد باتباع الخطوات التالية:

١- تحميل التطبيق من أي متجر كـ Google Play أو Mobogenie أو Aptoid.

٢- تثبيت التطبيق على الجهاز.

٣- فتح التطبيق و الوصول إلى نافذة الخيارات Options.

٤- الضغط على خيار Full UnRoot وإعادة تشغيل الجهاز.

إن كان الـ Root من أصل الـ ROM فمن الممكن تفعيل خيار Disable أو استعادة الـ ROM الأصلية أو تثبيت أخرى غير حاوية على Root.

Results

شكّل الـ Root حلّاً للكثير من المشكلات التي أعاقت مستخدمي الـ Android:

- ❖ أتاح للمستخدم الوصول لأي ملف متعلّق بالنظام مع إمكانية التعديل بالتّالي تصحيح الأخطاء الموجودة في كل نسخة Android قديمة كانت أم جديدة.

- ❖ وصل بالجهاز إلى أقصى الحدود (Overclocking).

- ❖ زاد الـ Root من فترة خدمة الجهاز، عبر إمكانيّة التحديث لآخر نسخ الـAndroid.

- ❖ سهّل عمليّة أخذ النسخ الاحتياطية ووصل بها إلى أخذ نسخ احتياطية عن نظام.

- ❖ سمح بنقل معلومات التطبيقات إلى بطاقة الذاكرة.

مع كل الخطورة التي يتعرض لها المستخدم جرّاء الـ Root إلّا أنّنا وجدنا حلاً لكلّ مشكلة تقريباً.

Conclusion

في هذا البحث طرقنا موضعاً شائعاً في عالم الأندرويد هو الـ Root ؛ **موضوع جذب الكثير من المستخدمين متأملين الحصول على قدرات الـ** Superman **في أجهزتهم فتحدّثنا عن ماهيّته .**

وضّحنا إيجابياته فلاحظنا أنّها لا تعدّ ولا تحصى ، و لم ننسَ سلبياته و مخاطره التي حالت بابتعاد الكثيرين عن الـ Root **خوفاً على أجهزتهم ، فلم نتوقف هنا بل حاولنا حل جميع المشاكل الممكنة الحدوث .**

تناولنا العديد و العديد من تطبيقات الـ Root **فلاحظنا الفرق من أداء الجهاز حتّى التحكم بكلّ التطبيقات بالإضافة للتهرّب من الدفع بعد الفترة التجريبية و لن ننسى أهميته في الاختراق و تحديداً اختراق الشبكات .**

و في النهاية كان موضوعنا كيفية عمل Root **للجهاز أو التراجع عنه.**

لقد طرقنا موضوعاً جديداً نسبياً و قمنا بفتح باب واسع أمام المستخدم و في نهاية بحثي هذا كل ما سأقوله :

Figures' Table

الموضوع	رقم الصفحة	رقم الشكل
Android OS	٢	الشكل (١،١،١)
الحواجز و الإعاقات بدون الـ Root	٤	الشكل (٢،١،١)
Unix OS	٥	الشكل (١،٢،١)
Linux OS	٥	الشكل(٢،٢،١)
آليّة عمل الـ Root	٦	الشكل(٣،٢،١)
فوائد و إيجابيات الـ Root	٧	الشكل (١،١،٢)
Stock Recovery	١٠	الشكل (٢،١،٢)
Clockwork Mod Recovery	١٠	الشكل (٣،١،٢)
Team Win Recovery	١٠	الشكل (٤،١،٢)
لماذا تقوم بالـ Root	١١	الشكل (٥،١،٢)
مخاطر و سلبيات الـ Root	١٢	الشكل(١،٢،٢)
تطبيقات الـ Root	١٥	الشكل(١،٤،٢)
SET CPU	١٥	الشكل(٢،٤،٢)
RAM Manager Pro	١٦	الشكل(٣،٤،٢)
Game Killer	١٦	الشكل(٤،٤،٢)
WiFi Kill	١٧	الشكل(٥،٤،٢)
GL To SD Card	١٧	الشكل(٦،٤،٢)
Disk digger	١٨	الشكل(٧،٤،٢)
zANTI	١٨	الشكل(٨،٤،٢)
Triangle Away	١٩	الشكل(٩،٤،٢)
Wps Wpa Tester	١٩	الشكل(١٠،٤،٢)

Sources and References

A.Heger, D. "Mobile Devices - An Introduction to the Android Operating Environment-
Design, Architecture, and Performance Implications." DHTechnologies.

Cordora, A. (2013). Take Control: The Android Rooting Guide, tig3r0nz.

Singh, R. (Feb 2014). Engineering Research and Applications **1**.

Tamma, R. and D. Tindall (2015). Learning Android Forensics, Packt Publishing.

Tyler, J. and W. Verduzco (2012). XDA Developers' Android Hacker's Toolkit: The Complete Guide to Rooting, ROMs and Theming, Wiley.

.