Rooteo en Android

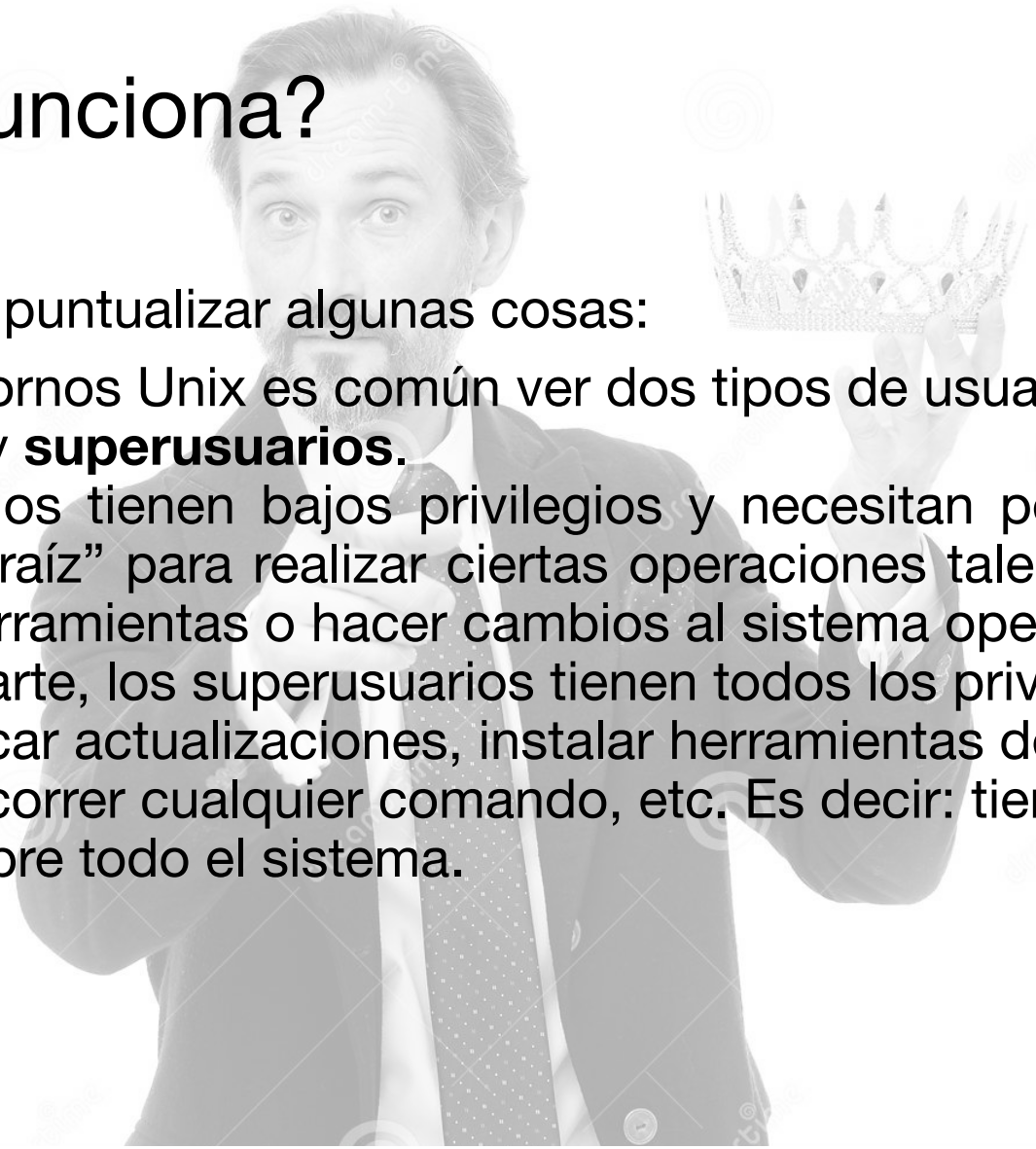
Rivera García Mauricio
Ruiz Flores Laura Andrea

A rasgos generales, ¿qué es?

- Es una técnica que permite a un usuario de Android tener un control privilegiado del equipo.
- De forma predeterminada, los dispositivos Android no tienen estos privilegios activados, pero es posible acceder a ellos en ciertos escenarios.
- Se le conoce también como el “superusuario”

Rivera García Mauricio
Ruiz Flores Laura Andrea

¿Cómo funciona?



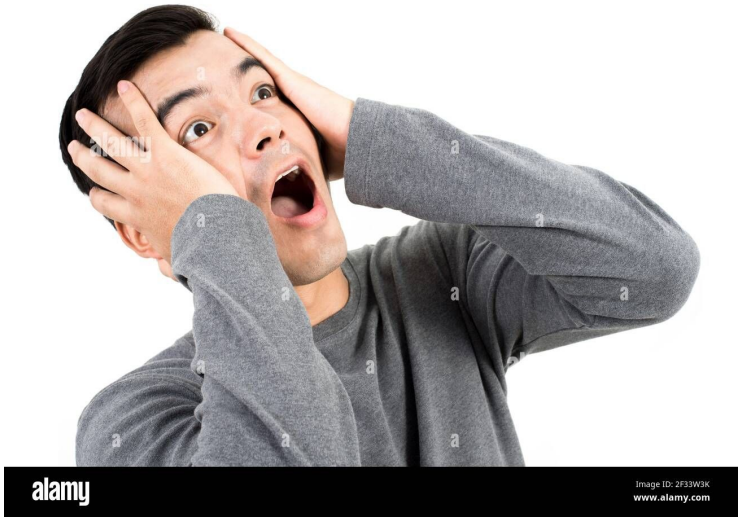
Es importante puntualizar algunas cosas:

- En los entornos Unix es común ver dos tipos de usuario: **usuarios** y **superusuarios**.
- Los usuarios tienen bajos privilegios y necesitan permisos desde la “raíz” para realizar ciertas operaciones tales como instalar herramientas o hacer cambios al sistema operativo.
- Por otra parte, los superusuarios tienen todos los privilegios como aplicar actualizaciones, instalar herramientas de software, correr cualquier comando, etc. Es decir: tiene un control sobre todo el sistema.

Rivera García Mauricio
Ruiz Flores Laura Andrea

- Entonces cabe mencionar que Android es, de hecho, un sistema operativo basado en el kernel de Linux.
- Esto implica que muchas de las cosas que se ven en los sistemas Linux tradicionales se pueden ver también en los sistemas Android, como lo es esta separación de privilegios.
- Pero, como se dijo antes, en Android no puedes acceder a este modo desde el prinicipio.

Es decir que, técnicamente, no eres el dueño de tu dispositivo



Rivera García Mauricio
Ruiz Flores Laura Andrea

Entonces, el rooteo trata de obtener total control sobre tu dispositivo Android.

Rivera García Mauricio
Ruiz Flores Laura Andrea

Pero…

Es importante mencionar los mecanismos de protección que tiene Android sobre algunos métodos de rooteo.

Rivera García Mauricio
Ruiz Flores Laura Andrea

Cabe mencionar…

El procedimiento puede ser un tanto complicado y frustrante.

Rivera García Mauricio
Ruiz Flores Laura Andrea

Bootloader

- Es de los primeros pedazos de código en ser ejecutados al arrancar el dispositivo.
- En este punto se arranca el sistema operativo, por lo que con cierta configuración de teclas se podría acceder ahí y llegar a un Recovery System.
- Para dispositivos Android, se puede decir que el bootloader puede estar bloqueado o desbloqueado.

Rivera García Mauricio
Ruiz Flores Laura Andrea

Recovery System

- Siendo ejecutado por el bootloader, el sistema de recuperación tiene un control total sobre todo el sistema.
- En este punto es donde básicamente se puede acceder a una versión alternativa del sistema operativo, por lo general **aprobada por el fabricante.** Esto depende de si el bootloader esta bloqueado o no.

Cuando está bloqueado, sólo permite arrancar las versiones del sistema que el fabricante instale, asegurándose que el móvil no pueda ser manipulado.

Si está bloqueado, entonces no se puede rootear el dispositivo mediante el Bootloader :(

Rivera García Mauricio
Ruiz Flores Laura Andrea

adb shell

- Android Debug Bridge (ADB) es una linea de comandos que permite acceder a una “shell” de Android a través de una PC o una Mac.
- A través de esta shell, se puede ejecutar varios comandos.
- Pero, **dependiendo de ciertos parámetros**, solo se pueden ejecutar ciertos comandos.

Rivera García Mauricio
Ruiz Flores Laura Andrea

- **¿dependiendo de ciertos parámetros?**

`ro.secure`

```
root@Obi_S454:/system/etc/permissions # getprop ro.secure
0
```

Si **`ro.secure=0`** *entonces se puede ejecutar cualquier comando en ADB con privilegios de superusuario*

```
walleye:/ # getprop ro.secure
1
```

Si **`ro.secure=1`** *los comandos se ejecutarán como un usuario sin privilegios de superusuario*

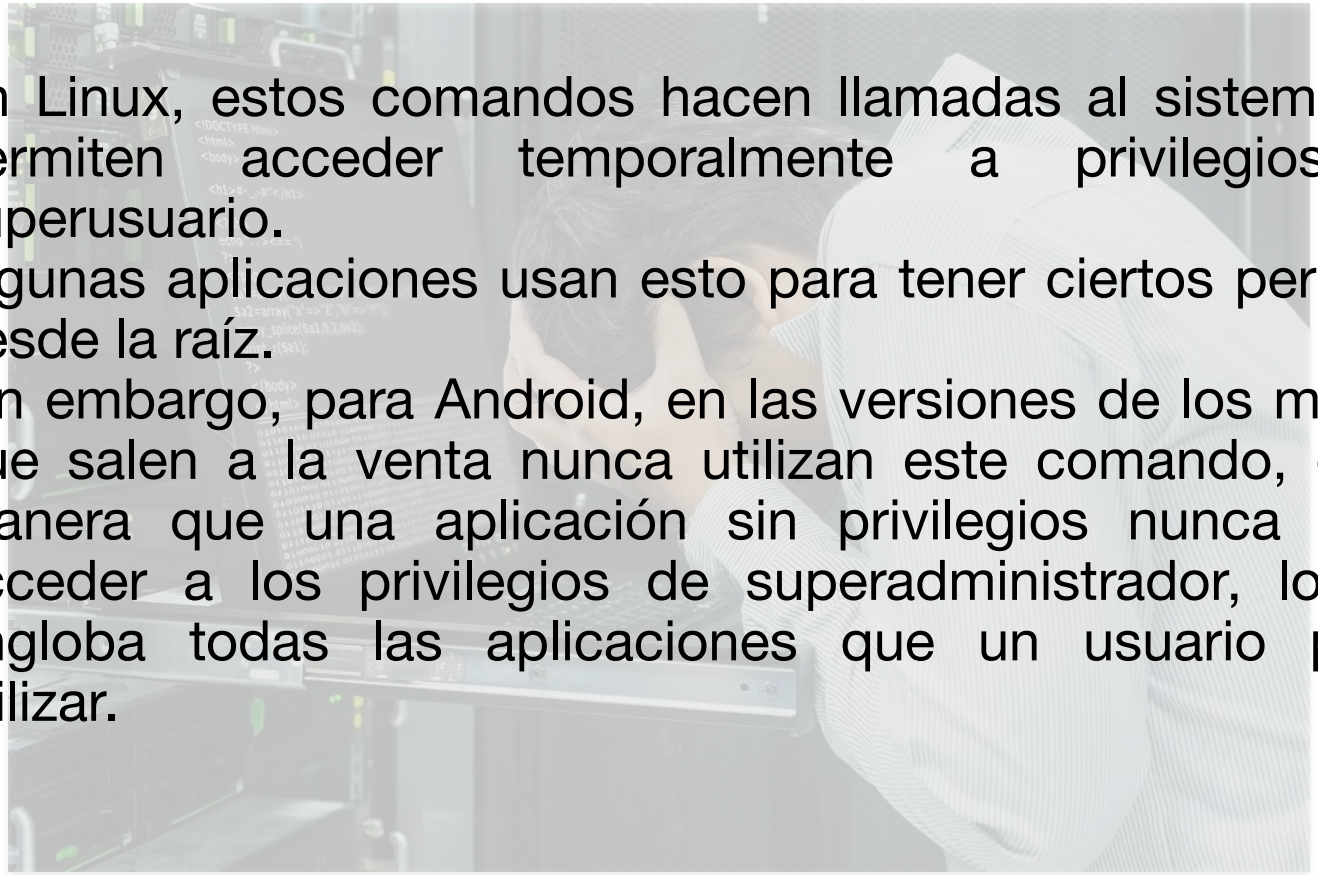
Rivera García Mauricio
Ruiz Flores Laura Andrea

Pero no es posible pasar el ro.secure de uno a cero

Si está en 1, entonces no se puede hackear el dispositivo mediante ADB :(

Rivera García Mauricio
Ruiz Flores Laura Andrea

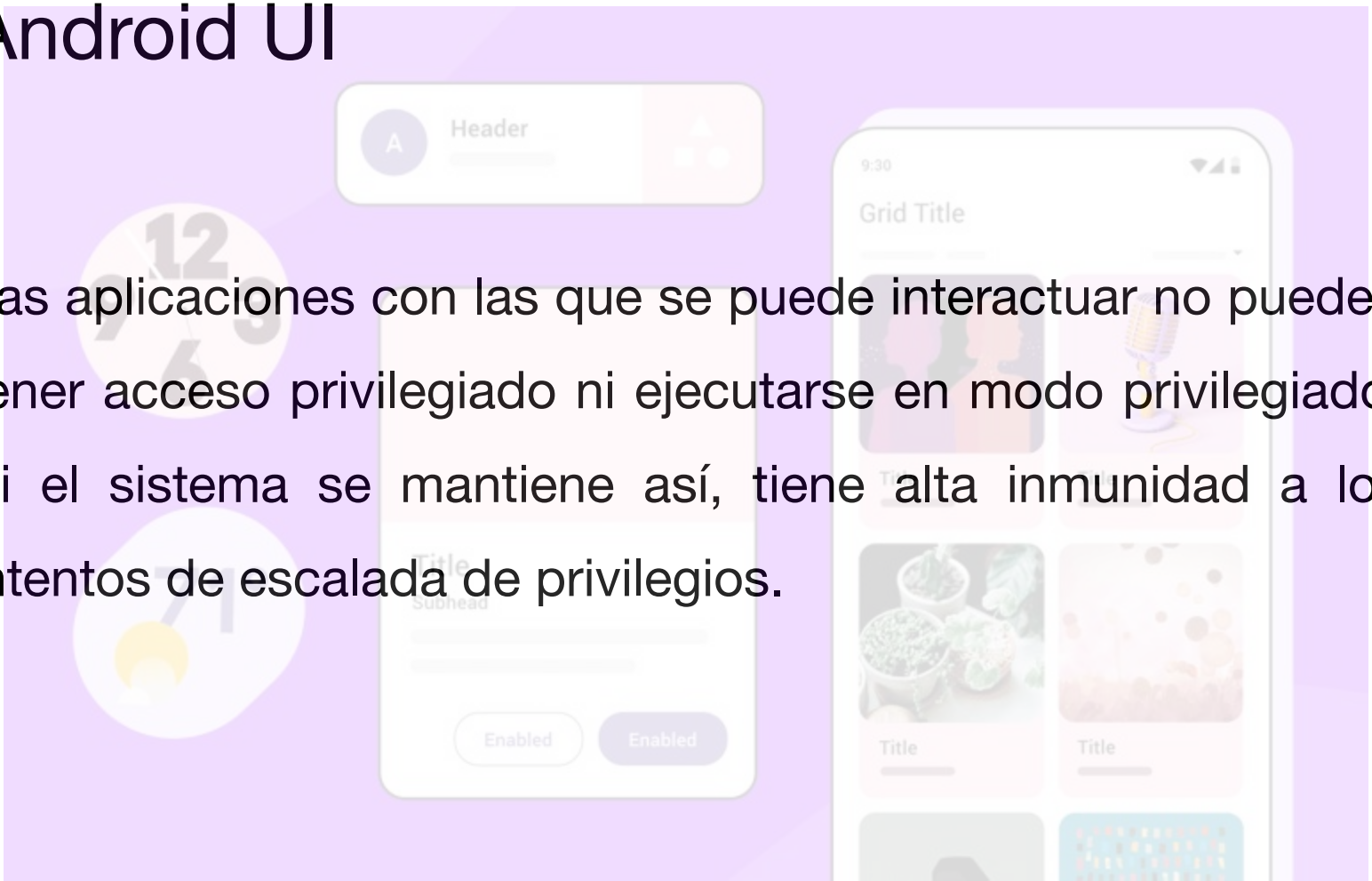
su y **sudo**



- En Linux, estos comandos hacen llamadas al sistema que permiten acceder temporalmente a privilegios de superusuario.
- Algunas aplicaciones usan esto para tener ciertos permisos desde la raíz.
- Sin embargo, para Android, en las versiones de los móviles que salen a la venta nunca utilizan este comando, de tal manera que una aplicación sin privilegios nunca podrá acceder a los privilegios de superadministrador, lo cual engloba todas las aplicaciones que un usuario puede utilizar.

Rivera García Mauricio
Ruiz Flores Laura Andrea

Android UI



Las aplicaciones con las que se puede interactuar no pueden tener acceso privilegiado ni ejecutarse en modo privilegiado. Si el sistema se mantiene así, tiene alta inmunidad a los intentos de escalada de privilegios.

Rivera García Mauricio
Ruiz Flores Laura Andrea

Escalada de Privilegios (Privilege Escalation)

Consiste en realizar un exploit o aprovechar una debilidad en el diseño del sistema operativo con la finalidad de tener acceso privilegiado a las aplicaciones del sistema.

Rivera García Mauricio
Ruiz Flores Laura Andrea

Su objetivo es:

- Leer y escribir archivos
- Persistir fácilmente entre reinicios
- Colocar una backdoor permanente

Se realiza a través de `su` y `sudo`.

Son capaces de ejecutar la llamada del sistema `setuid(0)`

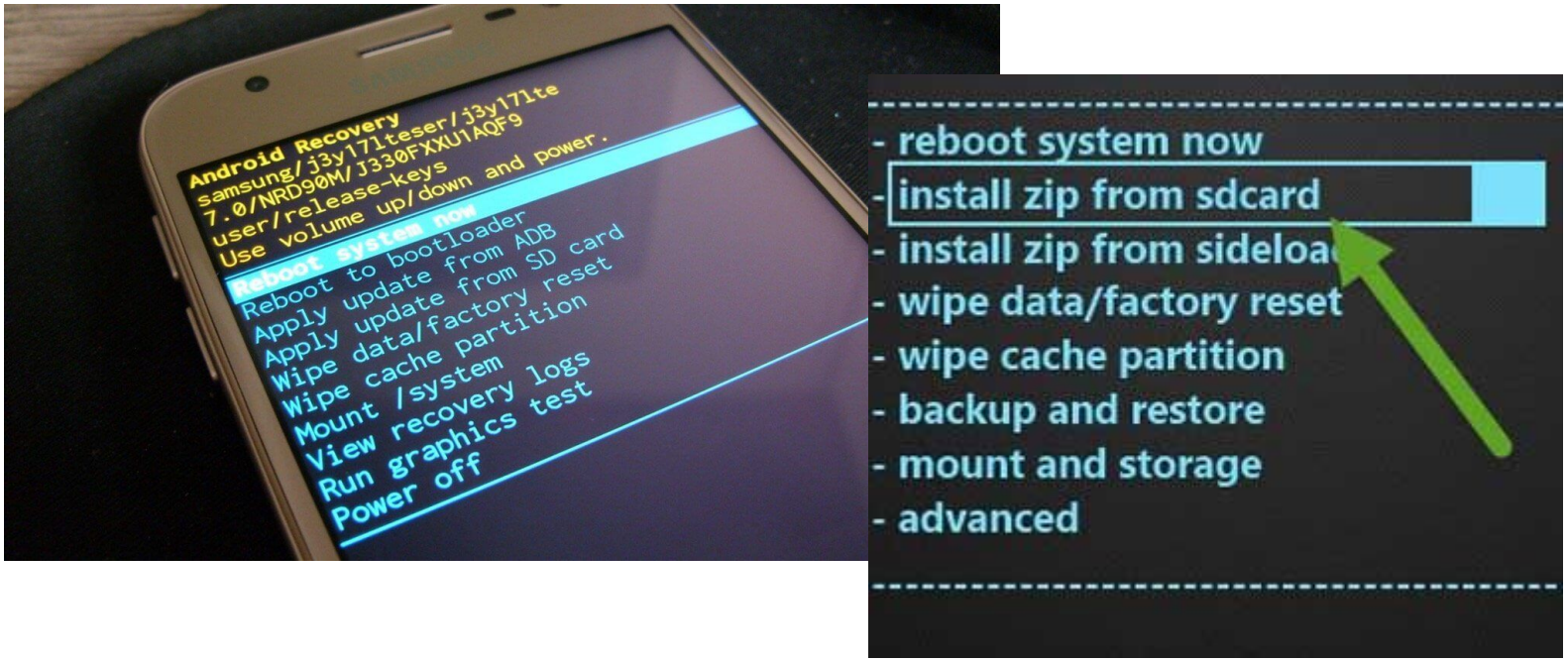
Rivera García Mauricio
Ruiz Flores Laura Andrea

Con todas estas restricciones, ¿cómo se realiza entonces el rooteo?

Rivera García Mauricio
Ruiz Flores Laura Andrea

El caso “fácil”

- El bootloader esta desbloqueado.
  - Básicamente, lo único que se necesita es realizar cierta combinación de teclas, obtener la configuración deseada y ejecutarla desde el bootloader y el sistema de recuperación.



Rivera García Mauricio
Ruiz Flores Laura Andrea

El caso ‘aún más fácil’

- **`ro.secure=0`**
  - En este caso, solo se requiere conectar el móvil a la computadora, ejecutar ADB, montar **`/system`** en modo lectura-escritura, instalar **`su`** y con eso basta.

```
C:\Users\athakur\adt-bundle-windows-x86_64-20140321\adt-bundle-windows-x86_64-20
140321\sdk\platform-tools>adb shell
shell@android:/ $ su
su
root@android:/ # mount -o remount,rw /system
mount -o remount,rw /system
root@android:/ # ls -la /system/bin/sh
ls -la /system/bin/sh
lrwxr-xr-x root     shell              2012-10-29 14:13 sh -> mksh
root@android:/ # chmod 4755 /system/bin/sh
chmod 4755 /system/bin/sh
root@android:/ # ls -la /system/bin/mksh
ls -la /system/bin/mksh
-rwsr-xr-x root     shell      152012 2012-10-29 14:13 mksh
root@android:/ #
```


Rivera García Mauricio
Ruiz Flores Laura Andrea

El caso real

- El bootloader está bloqueado.
- **`ro.secure=1`**

Se hace uso de los procesos que corran en la raíz obligatoriamente

Rivera García Mauricio
Ruiz Flores Laura Andrea

```
C:\Windows\system32>adb shell ps
USER      PID   PPID  VSIZE  RSS     WCHAN    PC         NAME
root      1     0     760    392   ffffffff 00000000 S /init
root      2     0     0      0     ffffffff 00000000 S kthreadd
root      3     2     0      0     ffffffff 00000000 S ksoftirqd/0
root      5     2     0      0     ffffffff 00000000 S kworker/0:0H
root      7     2     0      0     ffffffff 00000000 S migration/0
root      8     2     0      0     ffffffff 00000000 S rcu_preempt
root      9     2     0      0     ffffffff 00000000 S rcu_bh
root      10    2     0      0     ffffffff 00000000 S rcu_sched
root      11    2     0      0     ffffffff 00000000 R migration/1
root      12    2     0      0     ffffffff 00000000 R ksoftirqd/1
root      14    2     0      0     ffffffff 00000000 S kworker/1:0H
root      15    2     0      0     ffffffff 00000000 R migration/2
root      16    2     0      0     ffffffff 00000000 R ksoftirqd/2
root      18    2     0      0     ffffffff 00000000 S kworker/2:0H
root      19    2     0      0     ffffffff 00000000 R migration/3
root      20    2     0      0     ffffffff 00000000 R ksoftirqd/3
root      22    2     0      0     ffffffff 00000000 S kworker/3:0H
root      23    2     0      0     ffffffff 00000000 S khelper
root      24    2     0      0     ffffffff 00000000 S suspend_sys_syn
root      25    2     0      0     ffffffff 00000000 S suspend
root      26    2     0      0     ffffffff 00000000 S writeback
root      27    2     0      0     ffffffff 00000000 S bioset
root      28    2     0      0     ffffffff 00000000 S kblockd
root      29    2     0      0     ffffffff 00000000 S khubd
root      48    2     0      0     ffffffff 00000000 S irq/322-charger
```


Rivera García Mauricio
Ruiz Flores Laura Andrea

- Hay muchos procesos que tienen que ser ejecutados desde root
- Entonces, la forma de rootear aprovecha estos procesos.

Básicamente, hay que modificar estos procesos para colar un código arbitrario entre ellos.

Código arbitrario que, casualmente, podría habilitar los permisos de superusuario en el sistema.

Y es así como nacen los “exploits” o “jailbreaks”

Rivera García Mauricio
Ruiz Flores Laura Andrea

Por listar algunos exploits…

- Exploid
- GingerBreak
- RageAgainstTheCage
- KillingInTheNameOf
- ZimperLich

Rivera García Mauricio
Ruiz Flores Laura Andrea

Ventajas

- Control ilimitado del dispositivo
- Instalación de apps adicionales
- Más características y opciones de personalización.

Rivera García Mauricio
Ruiz Flores Laura Andrea

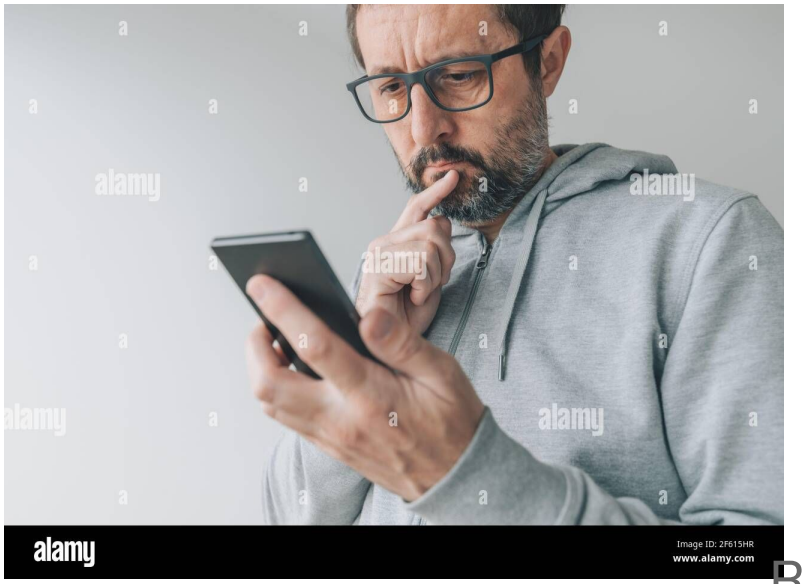
Desventajas

- Compromete la seguridad de tu dispositivo
- Brickeo del dispositivo
- Pérdida de la garantía

Rivera García Mauricio
Ruiz Flores Laura Andrea

Detección del rooteo

- Revisar los paquetes instalados.
- Revisar la existencia de archivos.
- Revisar procesos, servicios y tareas.
- Revisar comandos de ejecución de Shell.



Rivera García Mauricio
Ruiz Flores Laura Andrea

Sobre los fabricantes

Si el dispositivo tiene una afectación en el hardware por error de fábrica y no tiene relación con el rooteo, la garantía se puede seguir aplicando. Si el rooteo afecta el hardware, la garantía no será aplicada.

Con el descubrimiento de nuevos exploits, los fabricantes realizan parches para que en nuevos dispositivos se vuelvan inutilizables.

Rivera García Mauricio
Ruiz Flores Laura Andrea

Y ya

Rooteo en Android

Rivera García Mauricio
Ruiz Flores Laura Andrea

Referencias

Ji, Chuan. (2011) *How Rooting Works: A Technical Explanation of the Android Rooting Process*

Enlace:
https://jichu4n.com/posts/how-rooting-works-a-technical-explanation-of-the-android-rooting-process/

Srinivasa Rao Kotipalli y Mohammed A. Imran (2016) *Hacking Android.*

Enlace:

https://www.google.com.mx/books/edition/Hacking_Android/j86qDQAAQBAJ

Documentación de Android Debug Bridge (adb)

Enlace:

https://developer.android.com/studio/command-line/adb

Jon Oberheide y Zach Lanier (2011) *Don't Root Robots!*

Enlace:

https://jon.oberheide.org/files/bsides11-dontrootrobots.pdf

Rashid-Feroze. (2023). *Linux Privilege Escalation Guide.*

Enlace:

https://payatu.com/blog/a-guide-to-linux-privilege-escalation/

Luque S. (2016). *Los fabricantes, el root y la garantía, un mundo de confusión*

Enlace:

https://www.xatakandroid.com/sistema-operativo/los-fabricantes-el-root-y-la-garantia-un-mundo-de-confusion

Long Nguyen-Vu, Ngoc-Tu Chau, Seongeun Kang y Souhwan Jung. (2017) Android Rooting: An Arms Race between Evasion and Detection.

Enlace:

https://www.hindawi.com/journals/scn/2017/4121765/