Universidad del País Vasco
Euskal Herriko Unibertsitatea

Escuela Universitaria de Ingeniería Vitoria-Gasteiz
Ingeniaritzako Unibertsitate Eskola Vitoria-Gasteiz

Seguridad en dispositivos Android

VI Jornada de Seguridad y Protección de Datos de Carácter Personal

Escanéame

Pablo González Nalda

Depto. de Lenguajes y Sistemas Informáticos
EU de Ingeniería de Vitoria-Gasteiz

12 de noviembre de 2014

Modificado el 12 de noviembre de 2014

Contenidos de la presentación

Escuela Universitaria de Ingeniería Vitoria-Gasteiz
Ingeniaritzako Unibertsitate Eskola Vitoria-Gasteiz

Contenidos

Introducción

Por qué Android como estudio de Seguridad en entorno empresarial:

- Entorno móvil más usado, fácil de estudiar, software abierto (licencia Apache).
- Las amenazas son más importantes en Android por ser el sistema más usado y por ello poder extenderse como una epidemia (percolación).
- No hay un análisis profundo de los riesgos de las aplicaciones, incluso en la Play Store. Es un modelo contrario a iOS en el que el filtro no está en el sistema sino en la tienda de aplicaciones.

Introducción

Datos importantes:

- El móvil *inteligente* no es sólo personal y ocio, sino muy implantado en el entorno empresarial
- Es un sistema monousuario (aunque con ampliaciones para usuarios invitados)
- Amenazas de robar información sensible como agenda, datos personales (contactos teléfono, correo, domicilio), trayectoria GPS en el tiempo, relaciones sociales, datos bancarios, correo personal y laboral...
- Riesgos: *rooteo* o *jail breaking* es un riesgo si no se sabe. SuperSu para control de acceso a `root`
- El usuario debe responsabilizarse al instalar aplicaciones de otros repositorios o ROMs.

Contenidos

Arquitectura Android

Dos niveles:

- Kernel Linux y procesos del sistema en código nativo como cualquier *distro* Linux *
- Máquinas Virtuales Dalvik, cada una ejecuta una aplicación Android en Java. Son una *sandbox*. `JNI` permite crear aplicaciones en código nativo que encajan en los eventos y ciclo de vida de las aplicaciones Android.

* De hecho, se puede ejecutar una Debian estándar con `chroot` en *Lil' Debi*

Arquitectura Android

Permisos de usuarios

A cada **aplicación** se le asigna un nuevo y único **usuario** y **grupo** cuando se instala, por lo que no puede leer información de otros usuarios/aplicaciones durante su ejecución.

Ciertos permisos de las aplicaciones se gestionan con grupos Linux: por ejemplo, el usuario de una aplicación que se instale con el permiso de acceder a internet (o LAN) es agregado al grupo AID_NET.

Arranque de Android y Zygote

Arranque de Android y Zygote:

1. El proceso `init` de Linux lanza Zygote, que a su vez lanza la primera MV Dalvik.
2. El Zygote *hace fork* y su clon arranca el `System Server`, y éste crea todos los servicios.

Contenidos

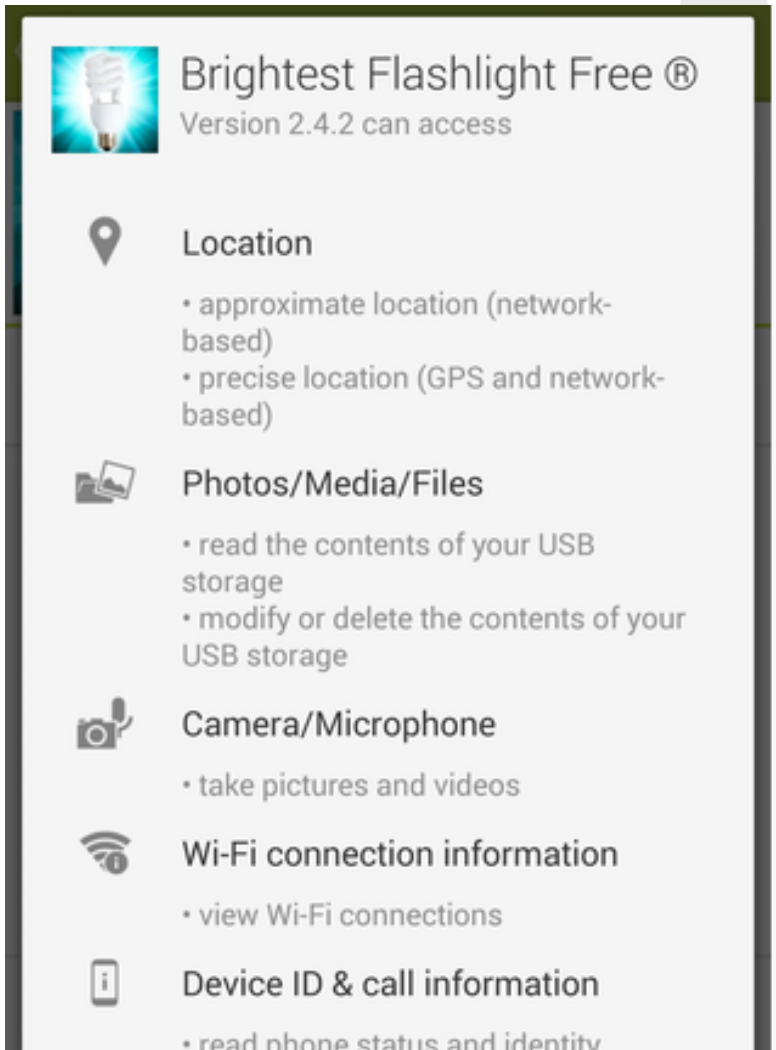
Modelos de Seguridad en Android: Kernel

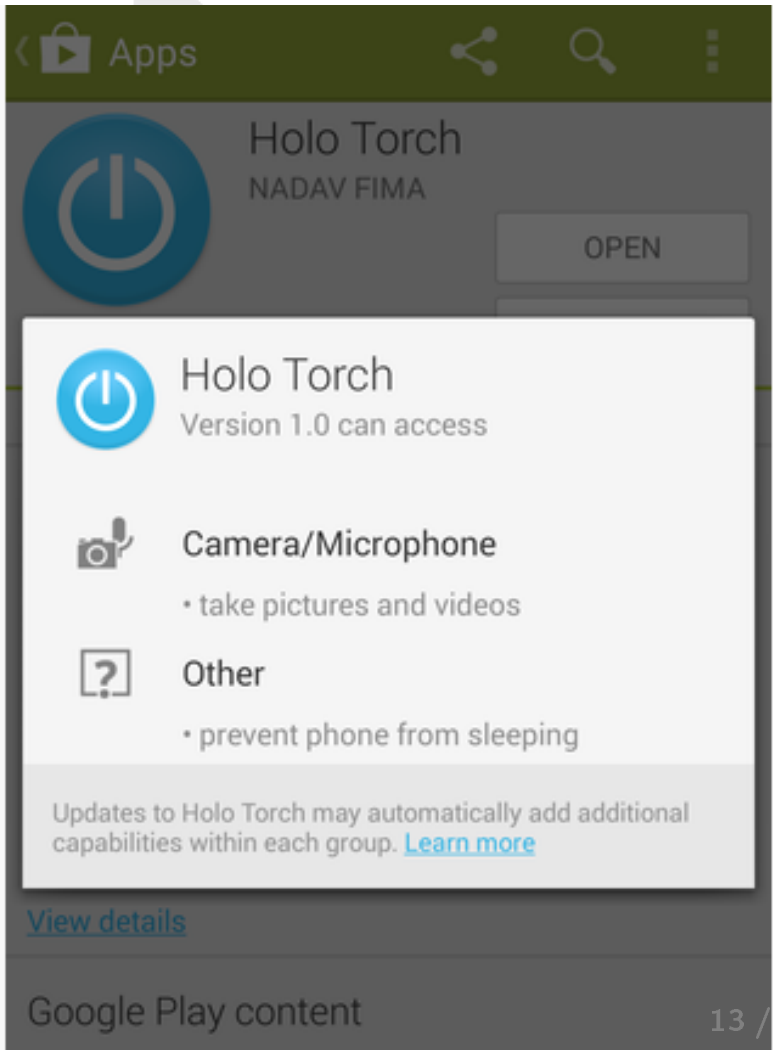
Android usa la seguridad en el nivel kernel con la ejecución de una aplicación como usuario.

Dos aplicaciones pueden compartir usuario y grupo e incluso proceso si están firmadas por la misma clave (al crear el fichero de instalación `apk`)

Modelos de Seguridad en Android: nivel *app*

En nivel aplicación, cada *app* define qué permisos necesita para las acciones que se necesitan.





Problemas de Seguridad en Android

En el momento de la instalación hay que aceptar todos permisos o no instalar.

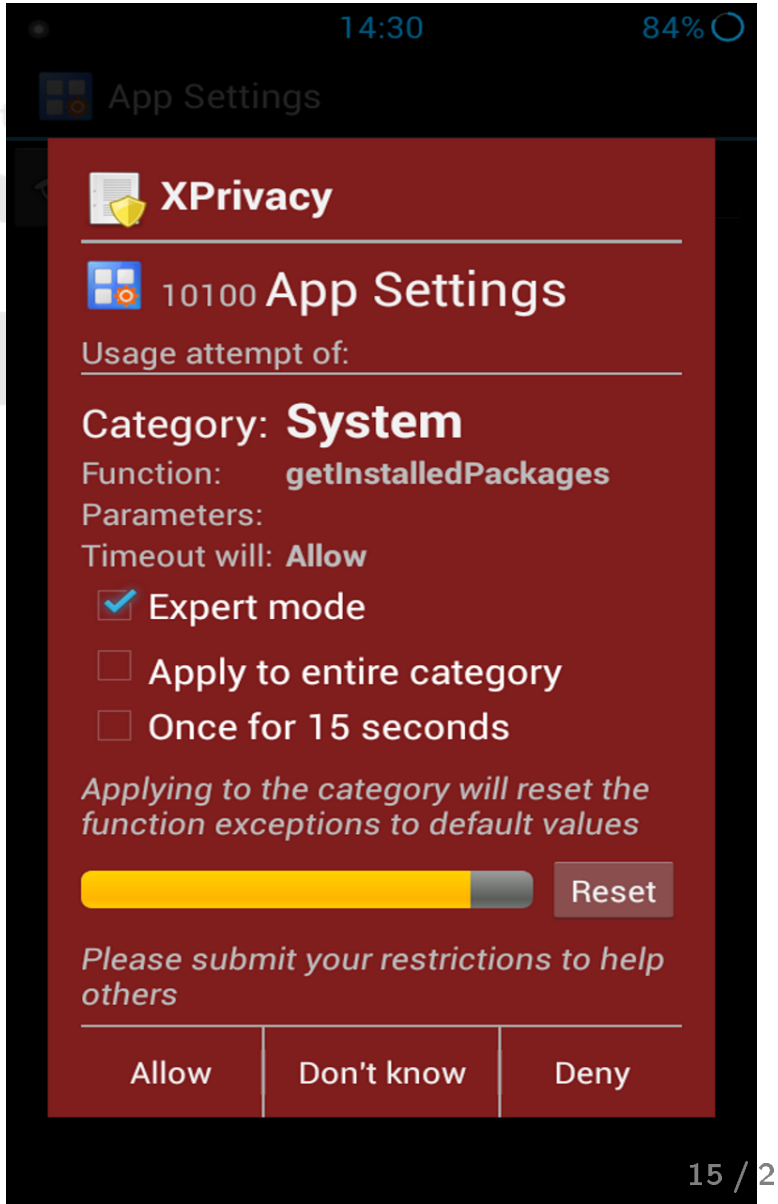
La sencillez de uso hace imposible aceptar en Android el uso de un recurso al intentar accederlo.

Soluciones:

1. Cyanogenmod (una variación del Android AOSP)
2. XPrivacy (una aplicación de Xposed Framework)
3. Un caso especial es el acceso a red, controlable con el cortafuegos de Linux y AfWall+.

XPrivacy

Contenidos



Riesgos de Seguridad en Android

Riesgos de Seguridad específicos de Android

1. pérdida o robo del móvil con sus datos o de una tarjeta de memoria, normalmente no encriptados.
2. Falta de privacidad con el teclado táctil e incluso con las manchas en la pantalla.
3. Anuncios y visitas a webs pueden informar de localización. Fichero `hosts` modificable con AdAway
4. Sistema Operativo Celular: SO para gestionar el acceso a la red GSM, la SIM, que suele ser antiguo y poco seguro por los problemas de modificarlo.
5. SELinux es un reforzamiento de reglas y permisos del Kernel.

Contenidos

Riesgos de Seguridad en la empresa con dispositivos móviles

Riesgos de Seguridad en la empresa con dispositivos móviles

Riesgo	Posible solución
Sin control sobre los dispositivos (robo o pérdida)	encriptar
Dispositivos no confiables (BYOD / Bring Your Own Device)	*sandbox*
Conexión a redes no confiables	VPN
Aplicaciones no confiables en dispositivos de empresa	educar y más políticas protectoras
Sincronización con sistemas externos, *"la nube"*	*Sandbox*
Contenido no confiable, de origen desconocido (QR con página maliciosa*, adjuntos)	antivirus y estar en alerta
Rastreo por GPS	Desconexión de GPS cuando sea posible
Falta de actualizaciones en sistema y aplicaciones	uniformizar dispositivos

* ¿Has escaneado el QR del inicio? Qué confianza...

Contenidos

Futuro de la Seguridad en la empresa con dispositivos móviles

Móviles de empresa con control remoto, Cyanogenmod, cortafuegos y control de permisos con XPrivacy

Google está aumentando la seguridad en Android, pero un móvil comprometido es un micrófono con GPS, cámara, filtrador de llamadas y todo tipo de comunicaciones.

Contenidos

Bibliografía

Bibliografía:

Android Security, Attacks and Defenses.
A. Dubey y A. Misra. CRC Press, 2013.

XPrivacy en el repositorio de Xposed Framework

AfWall+

Información de XPrivacy en GitHub

SELinux comentado por CyanogenMod

CyanogenMod en Wikipedia

eman ta zabal zazu

Universidad del País Vasco

Euskal Herriko Unibertsitatea

Escuela Universitaria de Ingeniería Vitoria-Gasteiz

Ingeniaritzako Unibertsitate Eskola Vitoria-Gasteiz

Escanéame

Seguridad en dispositivos Android

VI Jornada de Seguridad y Protección de Datos de Carácter Personal

Pablo González Nalda

Depto. de Lenguajes y Sistemas Informáticos
EU de Ingeniería de Vitoria-Gasteiz

12 de noviembre de 2014

Modificado el 12 de noviembre de 2014