SEGURINFO 2011

XI Congreso Interamericano de Seguridad de la Información

"SEGURIDAD, UNA PLATAFORMA DE VALOR PARA EL NEGOCIO"

DISPOSITIVOS MOVILES

¿Y AHORA QUÉ?

USUARIA

SEGURINFO 2011

XI Congreso Interamericano de Seguridad de la Información

"SEGURIDAD, UNA PLATAFORMA DE VALOR PARA EL NEGOCIO"

Presentada por:

Ezequiel Sallis
Director de I+D

Claudio Caracciolo
Director de SP

ROOT-SECURE
SECURITY MAKERS

Aclaración:

USUARIA

Agenda

- ✓ Situación Actual
- ✓ Problemática
  - Seguridad Física
  - Seguridad en Sistemas Operativos
  - Seguridad en Almacenamiento de Datos
  - Seguridad en Control de Accesos
  - Otros
- ✓ Contramedidas
- ✓ Demo
- ✓ Conclusiones

USUARIA

Situacion Actual (Deja-vu)

Los dispositivos móviles dejaron de ser únicamente un Gadget tecnológico para pasar a formar parte de un fenómeno social y empresarial.

Sus capacidades de procesamiento, usabilidad y conectividad se incrementan de manera vertiginosa.

Las redes de telefonía móvil que los soportan, han crecido tanto tecnológicamente como geográficamente permitiendo el acceso a la información en cualquier lugar de manera efectiva.

Tanto el acceso a la información corporativa como a contenidos sociales y ociosos se están mudando hacia la “cuarta pantalla” y los vectores de ataque tradicionales no son la excepción.

USUARIA

Situacion Actual

Por el contrario de lo que sucede con los sistemas operativos de las maquinas de escritorio, el mercado de los dispositivos móviles posee una mayor oferta y diversidad.

El mercado de los dispositivos móviles esta liderado por los smartphones pero las Tablets sin duda, jugaran un papel fundamental en las empresas en el corto plazo (si es que ya no lo están jugando ☺)

USUARIA

Situacion Actual - Actores principales

RIM OS (RIM)

IOS (Apple)

Android (Google)

Windows Mobile (Microsoft)

WebOS (HP)

Symbian

USUARIA

Problematica

Escenarios del mundo corporativo ante los dispositivos moviles

- ✓ Plataforma unica, integrada y estandarizada.
- ✓ Plaforma unica, integrada, estandarizada con excepciones.
- ✓ Plataforma IGWT *In God We Trust*

USUARIA

Problematica

Así como las notebooks fueron desplazando a las estaciones de trabajo, hoy en día los dispositivos móviles van ocupando ese lugar tan privilegiado. En la pelea por ocuparlo, los actores principales del mercado se enfocan en “la experiencia del usuario” trabajando en los temas de seguridad de manera reactiva.

USUARIA

Problemática – Seguridad Fisica

Como en los viejos tiempos, la perdida y/o el robo representan hoy en día el problema mas significativo.

En el mejor de los casos, solo deberíamos lamentar la perdida del hardware, de no ser así, es solo el principio del problema.

El escenario corporativo mas afectado es el IGWT ya que desconoce la existencia de los equipos en la red, de la información almacenada en el mismo (claves, datos, mails, etc) e incluso hasta de la perdida producida.

Problemática – Seguridad en Sistemas Operativos

La diversidad y segmentación (fragmentación) de los sistemas operativos disponibles para los dispositivos móviles plantea desde el inicio un complejo escenario:

- ✓ Administración de perfiles de multi-usuario
- ✓ Arquitectura de seguridad (basados en ID o Privilegios)
- ✓ Segmentación/fragmentación de versiones
- ✓ Gestión y remediación de vulnerabilidades

USUARIA

Problemática – Seguridad en Aplicaciones

Si bien existe multiplicidad de problemas a nivel aplicación, quizás la forma mas clara de representarla se resuma en estos cuatro ítems:

- ✓ Ausencia de buenas practicas de desarrollo seguro
- ✓ Errores de diseño (Usabilidad vs Seguridad)
- ✓ Instalación de software no controlado (legal e ilegal)
- ✓ Firmado de aplicaciones
- ✓ Malware
- ✓ Canales de comunicación inseguros

Problemática – Seguridad en Aplicaciones

DEMO

USUARIA

Problemática – Seguridad en Almacenamiento de Datos

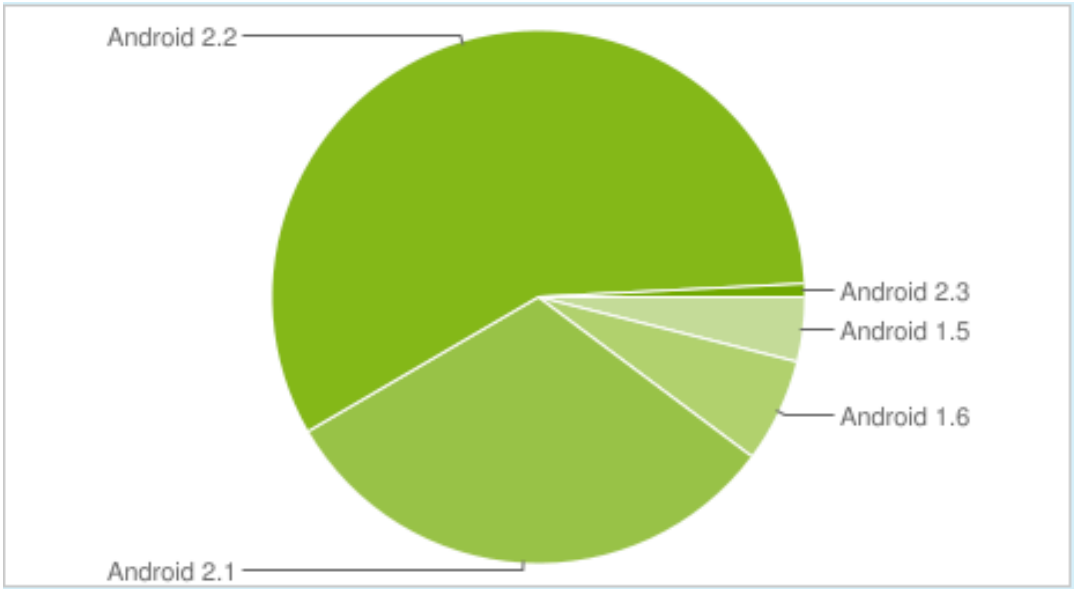
La mayoría de los dispositivos móviles poseen mas de una zona donde almacenar los datos, independientemente de su arquitectura. Todos los actores están de acuerdo en que deben protegerlos, sin embargo no todos lo hacen de la misma forma:

- ✓ Cifrado a nivel de RAM
- ✓ Cifrado a nivel de ROM
- ✓ Cifrado a nivel de Memoria de Local
- ✓ Cifrado a nivel de Memoria de Almacenamiento Extraible (SD)

Problemática – Seguridad en Almacenamiento de Datos

USUARIA

Problemática – Seguridad en Almacenamiento de Datos



Platform	API Level	Distribution
Android 1.5	3	3.9%
Android 1.6	4	6.3%
Android 2.1	7	31.4%
Android 2.2	8	57.6%
Android 2.3	9	0.8%

Data collected during two weeks ending on February 2, 2011

USUARIA

Problemática – Seguridad en Control de Accesos

Muy relacionado con el acceso físico, y conformando la primer barrera de protección, el PIN o CLAVE se convierte en un factor primordial.

- ✓ Claves débiles (predictibilidad y tamaño)
- ✓ Teclados complejos para claves complejas
- ✓ Ingeniería social (shoulder surfing)
- ✓ Almacenamiento inseguro de claves en los dispositivos
- ✓ Ausencia de múltiples capas de validación.

Problemática – Seguridad en Control de Accesos

DEMO

USUARIA

Problemática – Otros aspectos relevantes

- ✓ 802.11
- ✓ Bluetooth
- ✓ 3G / EDGE / GSM
- ✓ USB / Mini USB / etc
- ✓ Privacidad (Geolocalización y Metadatos)

Contramedidas

Contramedidas

Definir estándares de seguridad independientemente de la plataforma.

Concienciación de usuarios.

Utilizar los sistemas de administración centralizada (Mobile Device Manager) para las plataformas implementadas:

- Habilitar borrado remoto.
- Habilitar bloqueo remoto.
- Geolocalización del equipo.
- Aplicación de Politicas (OTA)

Contramedidas

Robustecer controles de acceso según criticidad del dispositivo/dueño (Pin a nivel de OS, Pin a nivel de SIM, Medios Extraíbles, autenticación por aplicación y factor de autenticación múltiple)

Cifrado de la información (medios de almacenamiento locales, extraíbles y memorias).

USUARIA

Conclusiones

Los dispositivos móviles, son mas que una moda.

Administrarlos de manera descentralizada es como implementar parches maquina por maquina en nuestra red.

Si los usuarios no entienden el problema, las soluciones son poco viables.

Los problemas de seguridad ya los conocemos, solo se mudaron a otro escenario.

Igualmente recuerde…

Conclusiones

Es Argentino pero atiende en todas partes, las 24 hs.

Gracias por haber asistido a nuestra charla!

USUARIA

Para mayor información:

Claudio Caracciolo
Director de SP
ccaracciolo (at) root-secure.com
Twitter: @holesec

Ezequiel Sallis
Director de I+D
esallis (at) root-secure.com
Twitter: @simubucks

Los invitamos a sumarse al grupo “Segurinfo” en LinkedIn

USUARIA