Amenazas a la privacidad de los datos en dispositivos móviles inteligentes

Dr. Ing. Gustavo Betarte

Profesor Titular, Grado 5
Grupo de Seguridad Informática
Instituto de Computación, Facultad de Ingeniería
Universidad de la República, Uruguay

www.fing.edu.uy/~gustun

Seminario AEPD-RPID Privacidad, noviembre 2015

Plan

Plan

Plan

Plan

Plan

Plan

Contexto

Contexto

La tecnología

Contexto

La tecnología

- Smartphones y tabletas

Contexto

La tecnología

- Smartphones y tabletas
- Internet of Things (IoT)

Contexto

La tecnología

- Smartphones y tabletas
- Internet of Things (IoT)
- Wearables

Contexto

La tecnología

- Smartphones y tabletas
- Internet of Things (IoT)
- Wearables

Las amenazas

Contexto

La tecnología

- Smartphones y tabletas
- Internet of Things (IoT)
- Wearables

Las amenazas

- Existen hoy más de 1M de aplicaciones maliciosas

Contexto

La tecnología

- Smartphones y tabletas
- Internet of Things (IoT)
- Wearables

Las amenazas

- Existen hoy más de 1M de aplicaciones maliciosas
- Pruebas de concepto sobre ataques en la IoT son ya una realidad

Smartphone

Smartphone

- Dispositivo electrónico portable con características de teléfono móvil y computador

Smartphone

- Dispositivo electrónico portable con características de teléfono móvil y computador
- Provee, entre otras funcionalidades

Smartphone

- Dispositivo electrónico portable con características de teléfono móvil y computador
- Provee, entre otras funcionalidades
  - Comunicación oral, texto, videos

Smartphone

- Dispositivo electrónico portable con características de teléfono móvil y computador
- Provee, entre otras funcionalidades
  - Comunicación oral, texto, videos
  - Acceso al e-mail personal y de trabajo

Smartphone

- Dispositivo electrónico portable con características de teléfono móvil y computador
- Provee, entre otras funcionalidades
  - Comunicación oral, texto, videos
  - Acceso al e-mail personal y de trabajo
  - Acceso a Internet para comprar y manejar cuentas bancarias

Smartphone

- Dispositivo electrónico portable con características de teléfono móvil y computador
- Provee, entre otras funcionalidades
  - Comunicación oral, texto, videos
  - Acceso al e-mail personal y de trabajo
  - Acceso a Internet para comprar y manejar cuentas bancarias
- A diferencia de las computadoras u otros dispositivos siempre están con nosotros y muy raramente se apagan. Estudios indican que

Smartphone

- Dispositivo electrónico portable con características de teléfono móvil y computador
- Provee, entre otras funcionalidades
  - Comunicación oral, texto, videos
  - Acceso al e-mail personal y de trabajo
  - Acceso a Internet para comprar y manejar cuentas bancarias
- A diferencia de las computadoras u otros dispositivos siempre están con nosotros y muy raramente se apagan. Estudios indican que
  - 62 % de los usuarios no usan contraseña

Smartphone

- Dispositivo electrónico portable con características de teléfono móvil y computador
- Provee, entre otras funcionalidades
  - Comunicación oral, texto, videos
  - Acceso al e-mail personal y de trabajo
  - Acceso a Internet para comprar y manejar cuentas bancarias
- A diferencia de las computadoras u otros dispositivos siempre están con nosotros y muy raramente se apagan. Estudios indican que
  - 62 % de los usuarios no usan contraseña
  - usuarios tienen un 33 % más de probabilidad de ser víctimas de un hurto de identidad que personas que no usan este tipo de dispositivos

Información colectada y guardada por PdeS

Información colectada y guardada por PdeS

- Proveedores de servicio colectan información de los usuarios. No es común que detallen con precisión qué tipo de información y los motivos para hacerlo.

Información colectada y guardada por PdeS

- Proveedores de servicio colectan información de los usuarios. No es común que detallen con precisión qué tipo de información y los motivos para hacerlo.
- En el caso general, como mínimo

Información colectada y guardada por PdeS

- Proveedores de servicio colectan información de los usuarios. No es común que detallen con precisión qué tipo de información y los motivos para hacerlo.
- En el caso general, como mínimo
  - Llamadas entrantes y salientes: nros. origen y destino, duración

Información colectada y guardada por PdeS

- Proveedores de servicio colectan información de los usuarios. No es común que detallen con precisión qué tipo de información y los motivos para hacerlo.
- En el caso general, como mínimo
  - Llamadas entrantes y salientes: nros. origen y destino, duración
  - Mensajes entrantes y salientes: nros. origen y destino

Información colectada y guardada por PdeS

- Proveedores de servicio colectan información de los usuarios. No es común que detallen con precisión qué tipo de información y los motivos para hacerlo.
- En el caso general, como mínimo
  - Llamadas entrantes y salientes: nros. origen y destino, duración
  - Mensajes entrantes y salientes: nros. origen y destino
  - Cuán a menudo el usuario chequea el email o accede a la Internet

Información colectada y guardada por PdeS

- Proveedores de servicio colectan información de los usuarios. No es común que detallen con precisión qué tipo de información y los motivos para hacerlo.
- En el caso general, como mínimo
  - Llamadas entrantes y salientes: nros. origen y destino, duración
  - Mensajes entrantes y salientes: nros. origen y destino
  - Cuán a menudo el usuario chequea el email o accede a la Internet
  - Localización del usuario

Información colectada y guardada por PdeS

- Proveedores de servicio colectan información de los usuarios. No es común que detallen con precisión qué tipo de información y los motivos para hacerlo.
- En el caso general, como mínimo
  - Llamadas entrantes y salientes: nros. origen y destino, duración
  - Mensajes entrantes y salientes: nros. origen y destino
  - Cuán a menudo el usuario chequea el email o accede a la Internet
  - Localización del usuario
- Las políticas de retención de los datos varían según el PdeS

Información residente en el dispositivo a proteger

Información residente en el dispositivo a proteger

- Cualquier foto o video tomada desde el dispositivo

Información residente en el dispositivo a proteger

- Cualquier foto o video tomada desde el dispositivo
- Contenidos y detalles de emails y SMS enviados y/o recibidos

Información residente en el dispositivo a proteger

- Cualquier foto o video tomada desde el dispositivo
- Contenidos y detalles de emails y SMS enviados y/o recibidos
- Detalles de las llamadas: a/de quién? cuándo? cuánto tiempo?

Información residente en el dispositivo a proteger

- Cualquier foto o video tomada desde el dispositivo
- Contenidos y detalles de emails y SMS enviados y/o recibidos
- Detalles de las llamadas: a/de quién? cuándo? cuánto tiempo?
- Contactos

Información residente en el dispositivo a proteger

- Cualquier foto o video tomada desde el dispositivo
- Contenidos y detalles de emails y SMS enviados y/o recibidos
- Detalles de las llamadas: a/de quién? cuándo? cuánto tiempo?
- Contactos
- Contraseñas

Información residente en el dispositivo a proteger

- Cualquier foto o video tomada desde el dispositivo
- Contenidos y detalles de emails y SMS enviados y/o recibidos
- Detalles de las llamadas: a/de quién? cuándo? cuánto tiempo?
- Contactos
- Contraseñas
- Datos financieros

Información residente en el dispositivo a proteger

- Cualquier foto o video tomada desde el dispositivo
- Contenidos y detalles de emails y SMS enviados y/o recibidos
- Detalles de las llamadas: a/de quién? cuándo? cuánto tiempo?
- Contactos
- Contraseñas
- Datos financieros
- Contenido de calendarios

Información residente en el dispositivo a proteger

- Cualquier foto o video tomada desde el dispositivo
- Contenidos y detalles de emails y SMS enviados y/o recibidos
- Detalles de las llamadas: a/de quién? cuándo? cuánto tiempo?
- Contactos
- Contraseñas
- Datos financieros
- Contenido de calendarios
- Localización, edad, género

A quiénes les interesa nuestra información personal?

Criminales

- Hurto
- Malware
- Geotags

A quiénes les interesa nuestra información personal?

Criminales

- Hurto
- Malware
- Geotags

Anunciantes

- Apps
- Behavioral marketing, Targeting

A quiénes les interesa nuestra información personal?

Criminales

- Hurto
- Malware
- Geotags

Anunciantes

- Apps
- Behavioral marketing, Targeting

Gobiernos

- Forensia

Criminales

Criminales

Pérdida o hurto

Criminales

Pérdida o hurto

- Dinero

Criminales

Pérdida o hurto

- Dinero
- Usurpación de identidad

Criminales

Pérdida o hurto

- Dinero
- Usurpación de identidad
- Acoso

Criminales

Pérdida o hurto

- Dinero
- Usurpación de identidad
- Acoso

Malware

Criminales

Pérdida o hurto

- Dinero
- Usurpación de identidad
- Acoso

Malware

- Virus, Spyware, Troyanos, Gusanos (transmitidos por apps)

Criminales

Pérdida o hurto

- Dinero
- Usurpación de identidad
- Acoso

Malware

- Virus, Spyware, Troyanos, Gusanos (transmitidos por apps)
- Cantidad de ataques ha crecido sustancialmente gracias a la negligencia de los usuarios

Criminales

Pérdida o hurto

- Dinero
- Usurpación de identidad
- Acoso

Malware

- Virus, Spyware, Troyanos, Gusanos (transmitidos por apps)
- Cantidad de ataques ha crecido sustancialmente gracias a la negligencia de los usuarios

Geotags

Criminales

Pérdida o hurto

- Dinero
- Usurpación de identidad
- Acoso

Malware

- Virus, Spyware, Troyanos, Gusanos (transmitidos por apps)
- Cantidad de ataques ha crecido sustancialmente gracias a la negligencia de los usuarios

Geotags

- Información de geolocalización (GPS) embebidas, por ejemplo, en fotos tomadas por el usuario

Criminales

Pérdida o hurto

- Dinero
- Usurpación de identidad
- Acoso

Malware

- Virus, Spyware, Troyanos, Gusanos (transmitidos por apps)
- Cantidad de ataques ha crecido sustancialmente gracias a la negligencia de los usuarios

Geotags

- Información de geolocalización (GPS) embebidas, por ejemplo, en fotos tomadas por el usuario
- Fotos en Internet proveen información relevante acerca de los movimientos de un usuario

Anunciantes

Anunciantes

- Contar con información personal le permite a un anunciante conocer las preferencias de consumo que un usuario puede tener

Anunciantes

- Contar con información personal le permite a un anunciante conocer las preferencias de consumo que un usuario puede tener
- En la actualidad hay un gran variedad de aplicaciones (apps) que le permiten a un anunciante colectar/capturar datos de un dispositivo móvil

Anunciantes

- Contar con información personal le permite a un anunciante conocer las preferencias de consumo que un usuario puede tener
- En la actualidad hay un gran variedad de aplicaciones (apps) que le permiten a un anunciante colectar/capturar datos de un dispositivo móvil
- El problema de (pérdida de) privacidad se acentúa cuando esa información es compartida con terceros y combinada con otra información para crear un perfil de un usuario sin su consentimiento

Recolección y explotación de datos personales

Recolección y explotación de datos personales

Recolección

Recolección y explotación de datos personales

Recolección

- Anunciantes contratan y proveen código a desarrolladores de aplicaciones para acceder información de los usuarios

Recolección y explotación de datos personales

Recolección

- Anunciantes contratan y proveen código a desarrolladores de aplicaciones para acceder información de los usuarios
- Además de desplegar el anuncio el código colecta datos del dispositivo y los envia al anunciante o a una red de anuncios

Recolección y explotación de datos personales

Recolección

- Anunciantes contratan y proveen código a desarrolladores de aplicaciones para acceder información de los usuarios
- Además de desplegar el anuncio el código colecta datos del dispositivo y los envia al anunciante o a una red de anuncios
- Los datos colectados y/o compartidos pueden ser usados para crear un perfil detallado del usuario y venderlo al mejor postor

Recolección y explotación de datos personales

Recolección

- Anunciantes contratan y proveen código a desarrolladores de aplicaciones para acceder información de los usuarios
- Además de desplegar el anuncio el código colecta datos del dispositivo y los envia al anunciante o a una red de anuncios
- Los datos colectados y/o compartidos pueden ser usados para crear un perfil detallado del usuario y venderlo al mejor postor

Mercadeo comportamental

Recolección y explotación de datos personales

Recolección

- Anunciantes contratan y proveen código a desarrolladores de aplicaciones para acceder información de los usuarios
- Además de desplegar el anuncio el código colecta datos del dispositivo y los envia al anunciante o a una red de anuncios
- Los datos colectados y/o compartidos pueden ser usados para crear un perfil detallado del usuario y venderlo al mejor postor

Mercadeo comportamental

- Práctica de colectar y compilar registros de actividades, preferencias y/o localizaciones de un individuo

Recolección y explotación de datos personales

Recolección

- Anunciantes contratan y proveen código a desarrolladores de aplicaciones para acceder información de los usuarios
- Además de desplegar el anuncio el código colecta datos del dispositivo y los envia al anunciante o a una red de anuncios
- Los datos colectados y/o compartidos pueden ser usados para crear un perfil detallado del usuario y venderlo al mejor postor

Mercadeo comportamental

- Práctica de colectar y compilar registros de actividades, preferencias y/o localizaciones de un individuo
- Datos pueden ser analizados y combinados con otra información para crear perfiles muy detallados

Investigaciones policiales y legales

Investigaciones policiales y legales

- La capacidad de colectar información sobre las actividades de un individuo puede ser de un valor esencial para oficiales de la justicia

Investigaciones policiales y legales

- La capacidad de colectar información sobre las actividades de un individuo puede ser de un valor esencial para oficiales de la justicia
- Datos residentes en el dispositivo móvil de un individuo podrían ser utilizados en una corte como evidencia

Investigaciones policiales y legales

- La capacidad de colectar información sobre las actividades de un individuo puede ser de un valor esencial para oficiales de la justicia
- Datos residentes en el dispositivo móvil de un individuo podrían ser utilizados en una corte como evidencia
- La forensia de datos digitales residentes en dispositivos móviles se encuentra todavía en una etapa de desarrollo inicial, tanto técnico como legal

Spyware y Sniffing

Spyware y Sniffing

Spyware

Spyware y Sniffing

Spyware

- Un individuo que obtiene acceso físico a un dispositivo puede instalar software de vigilancia y monitoreo (spyware, por ejemplo), permitiendo:

Spyware y Sniffing

Spyware

- Un individuo que obtiene acceso físico a un dispositivo puede instalar software de vigilancia y monitoreo (spyware, por ejemplo), permitiendo:
- registrar y guardar las actividades del usuario en un archivo oculto en el dispositivo (posiblemente enviar la misma a un repositorio establecido)

Spyware y Sniffing

Spyware

- Un individuo que obtiene acceso físico a un dispositivo puede instalar software de vigilancia y monitoreo (spyware, por ejemplo), permitiendo:
- registrar y guardar las actividades del usuario en un archivo oculto en el dispositivo (posiblemente enviar la misma a un repositorio establecido)
- activar la cámara y el micrófono del dispositivo o trackear y registrar la localización del usuario

Spyware y Sniffing

Spyware

- Un individuo que obtiene acceso físico a un dispositivo puede instalar software de vigilancia y monitoreo (spyware, por ejemplo), permitiendo:
- registrar y guardar las actividades del usuario en un archivo oculto en el dispositivo (posiblemente enviar la misma a un repositorio establecido)
- activar la cámara y el micrófono del dispositivo o trackear y registrar la localización del usuario

Sniffing

Spyware y Sniffing

Spyware

- Un individuo que obtiene acceso físico a un dispositivo puede instalar software de vigilancia y monitoreo (spyware, por ejemplo), permitiendo:
- registrar y guardar las actividades del usuario en un archivo oculto en el dispositivo (posiblemente enviar la misma a un repositorio establecido)
- activar la cámara y el micrófono del dispositivo o trackear y registrar la localización del usuario

Sniffing

- Conexiones a Internet utilizando redes públicas Wi-Fi (o Bluetooth) pueden ser interceptadas permitiendo colectar información

Spyware y Sniffing

Spyware

- Un individuo que obtiene acceso físico a un dispositivo puede instalar software de vigilancia y monitoreo (spyware, por ejemplo), permitiendo:
- registrar y guardar las actividades del usuario en un archivo oculto en el dispositivo (posiblemente enviar la misma a un repositorio establecido)
- activar la cámara y el micrófono del dispositivo o trackear y registrar la localización del usuario

Sniffing

- Conexiones a Internet utilizando redes públicas Wi-Fi (o Bluetooth) pueden ser interceptadas permitiendo colectar información
- Los datos pueden ser lo que el usuario está escribiendo o información que está siendo colectada por una app que se está ejecutando en el dispositivo

Ingeniería social

Ingeniería social

- Cibercriminales abusan de la confianza de los usuarios convenciéndolos que los links, URLs, apps o archivos que les permiten montar los ataques son confiables

Ingeniería social

- Cibercriminales abusan de la confianza de los usuarios convenciéndolos que los links, URLs, apps o archivos que les permiten montar los ataques son confiables
- En 2014 se ha explotado fuertemente el poder de lo que se denomina *social proof*: la idea de que algo tiene más valor si es compartido o aprobado por otros

Ingeniería social

- Cibercriminales abusan de la confianza de los usuarios convenciéndolos que los links, URLs, apps o archivos que les permiten montar los ataques son confiables
- En 2014 se ha explotado fuertemente el poder de lo que se denomina *social proof*: la idea de que algo tiene más valor si es compartido o aprobado por otros
- Usuarios infravaloran sus datos siendo fácilmente convencidos de revelar voluntariamente direcciones de correo electrónico o credenciales de ingreso a cuentas sin verificar la que lo están haciendo en sitios web legítimos

El poder de las aplicaciones

El poder de las aplicaciones

- La popularidad y creciente disponibilidad y cantidad de apps descargables representa un problema mayor de privacidad

El poder de las aplicaciones

- La popularidad y creciente disponibilidad y cantidad de apps descargables representa un problema mayor de privacidad
- Se dedica más tiempo a usar las aplicaciones descargadas en los dispositivos móviles que en surfear la web

El poder de las aplicaciones

- La popularidad y creciente disponibilidad y cantidad de apps descargables representa un problema mayor de privacidad
- Se dedica más tiempo a usar las aplicaciones descargadas en los dispositivos móviles que en surfear la web
- Aplicaciones tan inocentes como lo son una *linterna*, una radio o un juego, colectan información del dispositivo, los contactos del usuario y/o su localización

El poder de las aplicaciones

- La popularidad y creciente disponibilidad y cantidad de apps descargables representa un problema mayor de privacidad
- Se dedica más tiempo a usar las aplicaciones descargadas en los dispositivos móviles que en surfear la web
- Aplicaciones tan inocentes como lo son una *linterna*, una radio o un juego, colectan información del dispositivo, los contactos del usuario y/o su localización
- Al instalar una aplicación es usual conceder permiso a acceder ciertos datos del dispositivo. La mayoría de las aplicaciones registran y monitorean la localización del usuario, información que es utilizada por servicios cuyo negocio depende de contar con ese tipo de información

El poder de las aplicaciones

- La popularidad y creciente disponibilidad y cantidad de apps descargables representa un problema mayor de privacidad
- Se dedica más tiempo a usar las aplicaciones descargadas en los dispositivos móviles que en surfear la web
- Aplicaciones tan inocentes como lo son una *linterna*, una radio o un juego, colectan información del dispositivo, los contactos del usuario y/o su localización
- Al instalar una aplicación es usual conceder permiso a acceder ciertos datos del dispositivo. La mayoría de las aplicaciones registran y monitorean la localización del usuario, información que es utilizada por servicios cuyo negocio depende de contar con ese tipo de información
- Los usuarios tendríamos que preguntárnos acerca de las aplicaciones que descargamos: quién las desarrolla?, qué datos colectan? dónde los guardan?, dónde envian la información?

El engaño y la privacidad en las redes sociales

El engaño y la privacidad en las redes sociales

- En el año 2014 el 70 % de las amenazas en medios sociales requirieron la colaboración de los usuarios finales para ser propagadas (en 2013 solamente el 2 %)

El engaño y la privacidad en las redes sociales

- En el año 2014 el 70 % de las amenazas en medios sociales requirieron la colaboración de los usuarios finales para ser propagadas (en 2013 solamente el 2 %)
- Mucha gente usa la misma contraseña en diferentes redes, lo que ha posibilitado a los cibercriminales poder explotar múltiples cuentas gracias a un solo hackeo

El engaño y la privacidad en las redes sociales

- En el año 2014 el 70 % de las amenazas en medios sociales requirieron la colaboración de los usuarios finales para ser propagadas (en 2013 solamente el 2 %)
- Mucha gente usa la misma contraseña en diferentes redes, lo que ha posibilitado a los cibercriminales poder explotar múltiples cuentas gracias a un solo hackeo

Vectores principales de ataque

El engaño y la privacidad en las redes sociales

- En el año 2014 el 70 % de las amenazas en medios sociales requirieron la colaboración de los usuarios finales para ser propagadas (en 2013 solamente el 2 %)
- Mucha gente usa la misma contraseña en diferentes redes, lo que ha posibilitado a los cibercriminales poder explotar múltiples cuentas gracias a un solo hackeo

Vectores principales de ataque

- Fake offering: este fraude consiste en invitar a usuarios de redes sociales a unirse a un falso grupo o evento ofreciendo incentivos como cuponeras gratis. Generalmente se requiere compartir credenciales con el atacante o enviar un texto a un nro. premium

El engaño y la privacidad en las redes sociales

- En el año 2014 el 70 % de las amenazas en medios sociales requirieron la colaboración de los usuarios finales para ser propagadas (en 2013 solamente el 2 %)
- Mucha gente usa la misma contraseña en diferentes redes, lo que ha posibilitado a los cibercriminales poder explotar múltiples cuentas gracias a un solo hackeo

Vectores principales de ataque

- Fake offering: este fraude consiste en invitar a usuarios de redes sociales a unirse a un falso grupo o evento ofreciendo incentivos como cuponeras gratis. Generalmente se requiere compartir credenciales con el atacante o enviar un texto a un nro. premium
- Fake Apps: usuarios finales son invitados a suscribirse a una aplicación que aparentemente puede integrar su uso a una red social, pero no solamente no hace lo que promete, sino que generalmente es usada para colectar credenciales u otros datos personales del usuario

Referencias

Symantec

ISTR 20: Internet Security Threat Report

http://www.symantec.com/threatreport, Volume 20, April 2015

Federal Trade Commission Staff Report

Mobile Privacy Disclosures: Building Trust Through Transparency

https://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf, February 2013

Privacy Rights ClearingHouse

10 Rules for Creating a Hacker-Resistant Password

https://www.privacyrights.org/ar/alertstrongpasswords.htm, September 2015

Privacy Rights ClearingHouse

Social Networking Privacy: How to be Safe, Secure and Social

https://www.privacyrights.org/social-networking-privacy, May 2015

Lifehacker

How to Stay Safe on Public Wi-Fi Networks

http://lifehacker.com/5576927/how-to-stay-safe-on-public-wi-fi-networks, November 2015