UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escola Tècnica Superior d'Enginyeria **Informàtica**

1. Riesgos para la seguridad en el ámbito móvil

Ciberseguridad en Dispositivos móviles
DISCA – ETS de Ingeniería informática (UPV)

Contenido

- Concepto de dispositivo móvil
- Fuentes de inseguridad: riesgos y vulnerabilidades en el ámbito móvil
- Situación actual

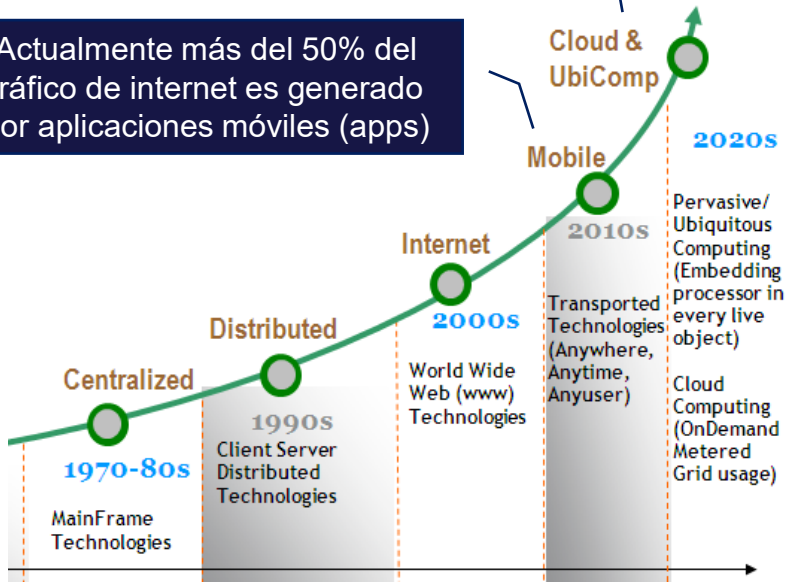
La computación ubícua

- Computación:
  - Realización de cálculos (rae)
- Móvil:
  - En movimiento (rae)
- Computación móvil:
  - Realización de cálculos en movimiento
- Computación ubícua:
  - … en todo momento y lugar

Evolución tecnológica

90% de la población mundial con acceso a Internet desde un dispositivo móvil

Actualmente más del 50% del tráfico de internet es generado por aplicaciones móviles (apps)



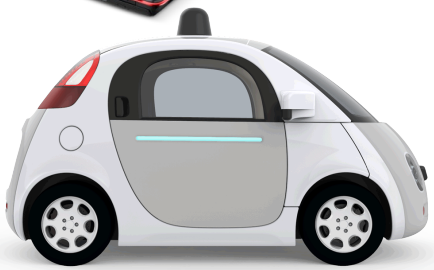
https://medium.com/@vivekmadurai/ubiquitous-computing-6dd3685f18e7

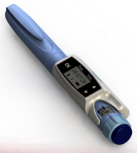
- Los últimos avances en materia de
  - Miniaturización y encapsulación
  - Comunicaciones inalámbricas
  - Manufactura de baterías

  (entre otros muchos) han hecho que el concepto de dispositivo móvil evoluciones y actualmente esté menos claro que nunca
- … aunque para casi todos hablar de dispositivos móviles es hablar de teléfonos inteligentes y tablets

¿Qué es un dispositivo móvil?

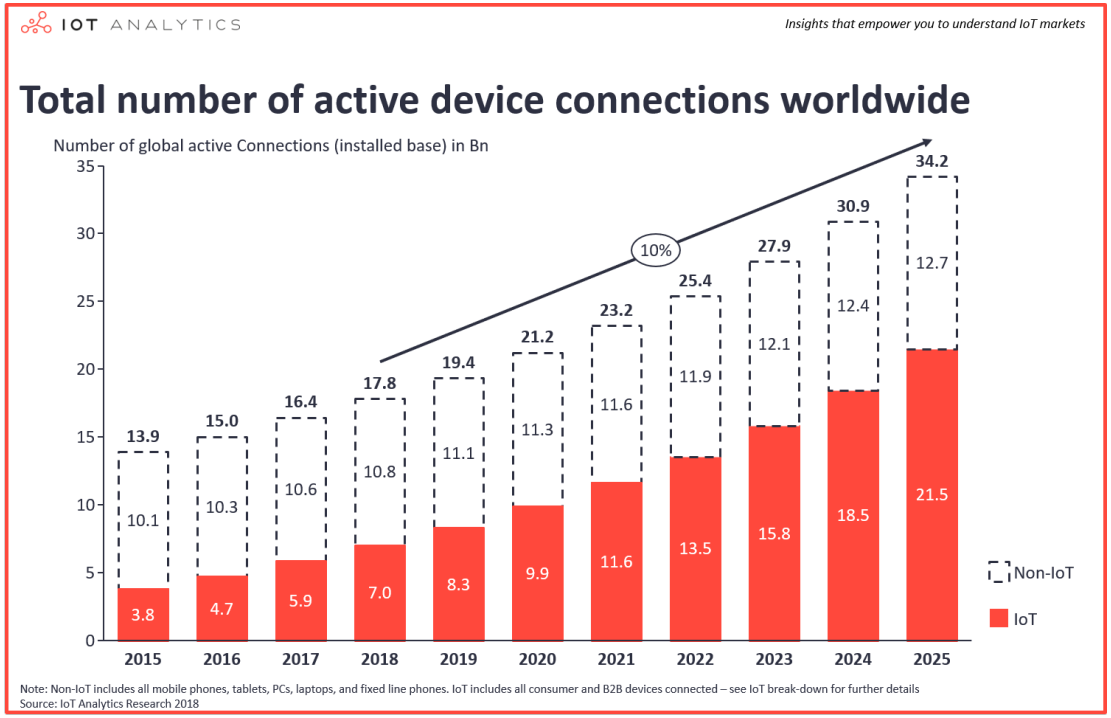
- ¿Qué lo diferencia?
  - Tamaño reducido → Movilidad y portabilidad
  - Autonomía (uso de batería → funcionalidad y capacidades limitadas)
  - Comunicaciones inalámbricas (conectividad no tiene por qué ser ni continua ni homogénea: 3/4G, bluetooth, WiFi, etc.)
  - Facilidad de uso → Interfaces M2M o H2M simples y adaptadas (pantallas táctiles, cámaras, puertos de comunicación, etc.)
  - Otras:
    - Multitud de sensores (acelerómetro, brújula digital y magnetómetro, barómetro, etc.)
    - Cámaras delantera y trasera
    - Geolocalización y posicionamiento (GPS, Glonass, Galileo, etc.)
    - Capacidades de actualización limitadas
    - ¿Vida útil más corta?
    - SW: Sistemas operativos y apps adaptados





Tendencias

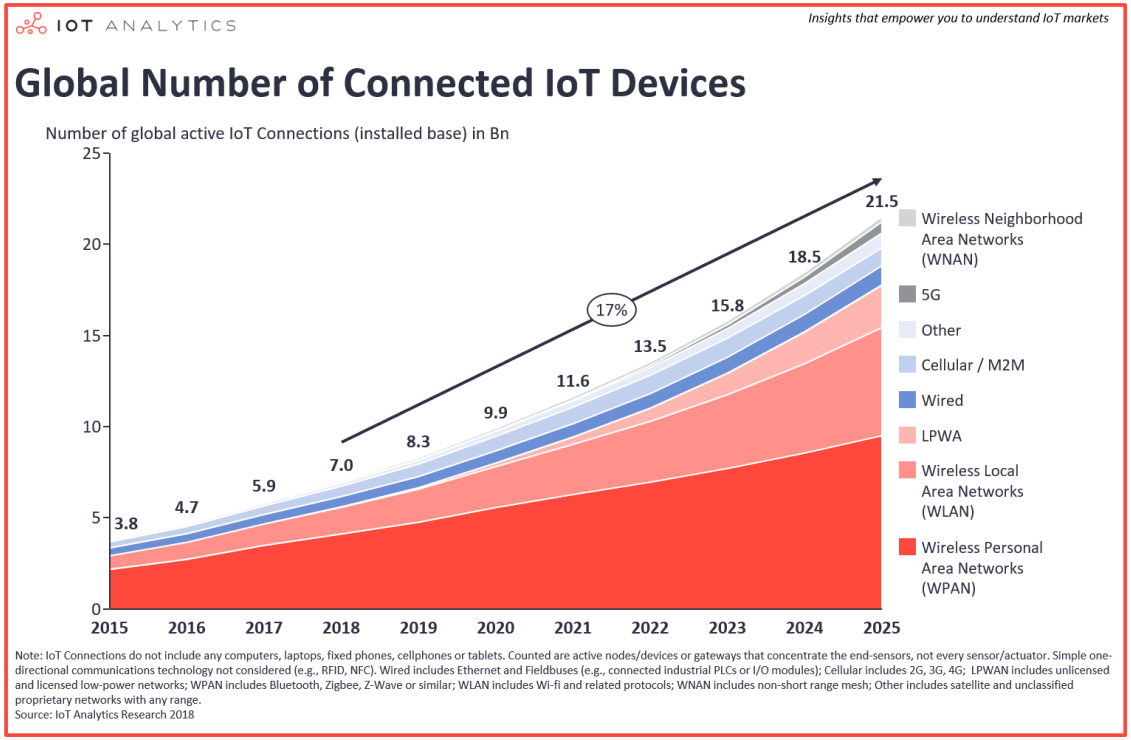
- Crecimiento anual del 10% del número de conexiones entre dispositivos



Fuente: Informe "State of the IoT 2018" (Agosto 2018)
Disponible en https://iot-analytics.com/product/state-of-the-iot-2018

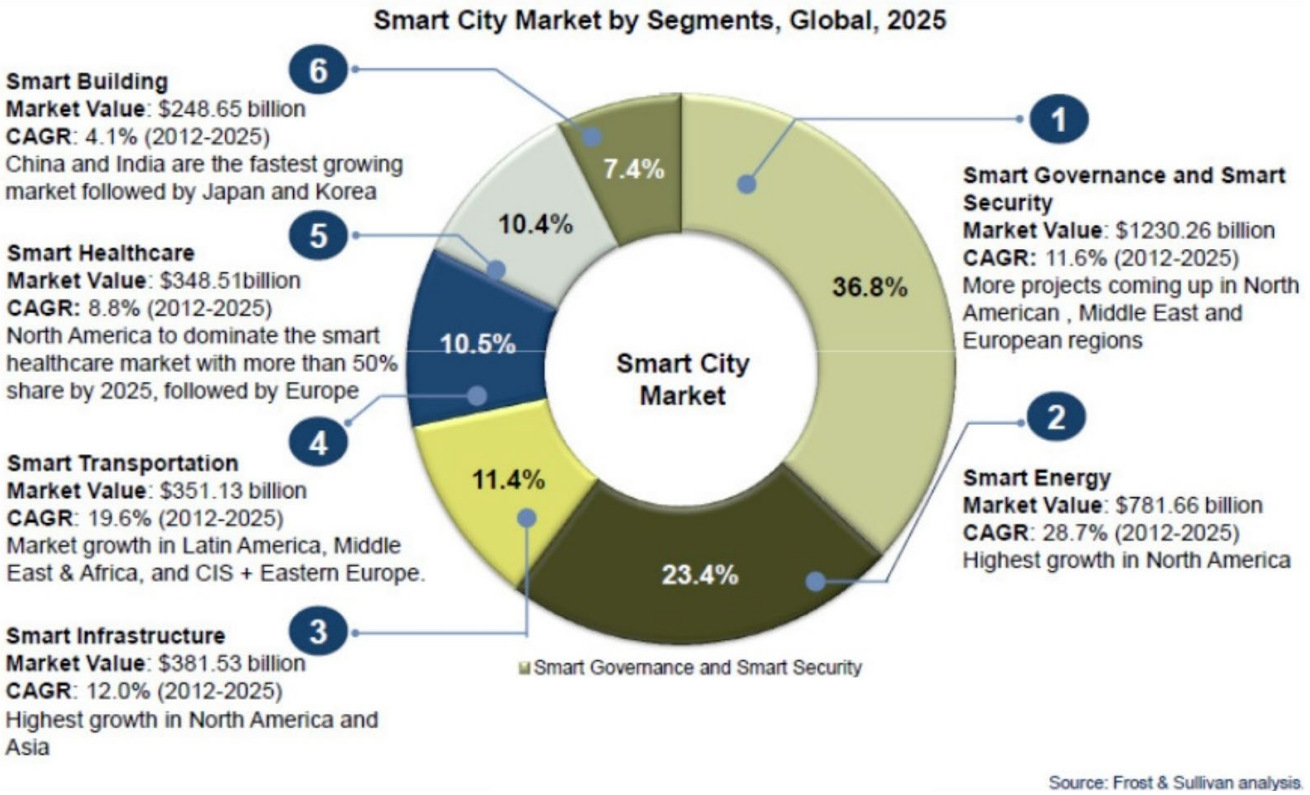
Tendencias

- Diversificación de las redes inalámbricas



Fuente: Informe “State of the IoT 2018” (Agosto 2018)
Disponible en https://iot-analytics.com/product/state-of-the-iot-2018

Potencial de mercado



Realidades tangibles

- Amazon go (automatización de supermercados)
  - https://www.youtube.com/watch?v=NrmMk1Myrxc
- Tesla full self-driving (conducción autónoma)
  - https://www.youtube.com/watch?v=0NtdZNWUBik
- Entrega de mercancías con drones (JDrone de Alibaba)
  - https://www.youtube.com/watch?v=3jiyzouhLNk
- La robótica móvil en la industria (almacenes de Amazon)
  - https://www.youtube.com/watch?v=Ox05Bks2Q3s

Contenido

- Concepto de dispositivo móvil
- **Fuentes de inseguridad: riesgos y vulnerabilidades en el ámbito móvil**
- Situación actual

Situación

- Gran potencial e interés de los dispositivos móviles para mejorar nuestro día a día → ¿Pero a costa de qué?
  - ¿Son vulnerables los dispositivos móviles y las apps que éstos ejecutan?
  - ¿Contienen información que pueda interesar a alguien?
- La respuesta a ambas preguntas es **Sí**
  - Vulnerabilidad + ataque = intrusión
  - Se necesita una intrusión para que se produzca una violación de una (o varias) política de seguridad
- Para garantizar la disponibilidad, integridad y confidencialidad de los activos que gestionan nuestros dispositivos debemos conocer los riesgos a los éstos están expuestos

Riesgos (1/6)

- Funcionalidad similar a los PCs → riesgos similares:
  - código malicioso
  - phishing
  - acceso a contenidos impropios u ofensivos
  - contacto con personas malintencionadas
  - pérdida de información
  - dificultad para proteger la privacidad
- Sus características los hacen incluso más atractivos a los ojos de los atacantes y las personas malintencionadas

Riesgos (2/6)

- Gran cantidad de información personal almacenada → Recolección indebida de:
  - mensajes SMS
  - listas de contactos
  - calendarios
  - historial de llamadas
  - fotos y videos
  - contraseñas
  - números de tarjetas de crédito
- Dispositivos que se reemplazan rápidamente sin eliminar debidamente la información almacenada

Riesgos (3/6)

- Mayor posibilidad de pérdida y robo
  - tamaño reducido
  - alto valor económico
  - símbolo de estatus
  - llaman la atención de los ladrones
  - se utilizan constantemente
  - se utilizan en lugares públicos
  - son fáciles de olvidar y perder

Riesgos (4/6)

- Invasión de la privacidad
  - Llevamos los dispositivos siempre con nosotros
    - Alguien podría tomarnos una fotografía y publicarla sin nuestro conocimiento o permiso
    - Grabar un audio sin nuestro consentimiento
    - Conocer nuestra localización
  - Exceso de información personal
    - lugares que frecuentamos
    - horarios, rutinas, hábitos
    - bienes personales
    - Recopilación de datos personales sin permiso y con objetivos maliciosos

Riesgos (5/6)

- Instalación de aplicaciones maliciosas
  - Gran cantidad de aplicaciones disponibles
    - diferentes autores
    - diferentes funcionalidades
    - dificultad para mantener el control
  - Algunas apps:
    - pueden no ser confiables
    - pueden tener errores de implementación
    - pueden haber sido específicamente desarrolladas para:
      - ejecutar actividades maliciosas
      - recoger datos de los dispositivos

Riesgos (6/6)

- Propagación de códigos maliciosos
  - códigos maliciosos recibidos a través de:
    - mensajes SMS
    - mensajes de correo electrónico
    - redes sociales, etc.
  - desde un dispositivo infectado se puede:
    - almacenar los datos recogidos
    - borrar los datos
    - participar de ataques en Internet
    - formar parte de botnets
    - contribuir a la diseminación de spam

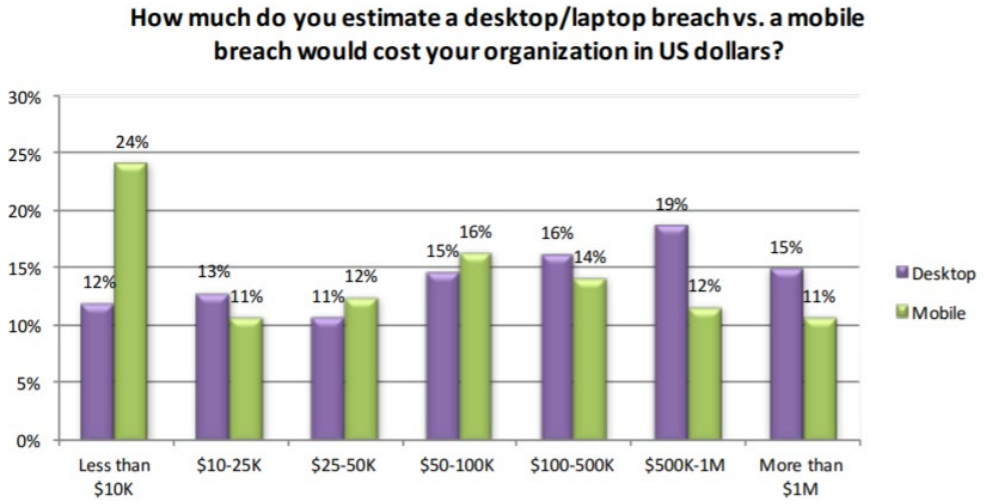
Impacto en el ámbito empresarial

- La omnipresencia de las TIC y las alternativas de movilidad existentes están abriendo la puerta a nuevas opciones de trabajo y productividad
- Bring Your Own Device (BYOD)
  - Los empleados tienen la posibilidad de llevar y utilizar sus propios dispositivos (ordenadores portátiles, smartphones, tabletas, wearables, etc.) en el trabajo y acceder desde ellos a los recursos de su compañía
  - Abaratamiento de costes por parte de la organización y aumento de la productividad
  - Implica la redefinición de gran parte de los procesos y métodos de trabajo, así como la revisión y adaptación de las políticas de seguridad
- Los ecosistemas móviles corporativos no pueden estar en riesgo ante ciberataques y la confidencialidad de la información que almacena toda una flota móvil debe ser protegida → La seguridad como pilar del BYOD

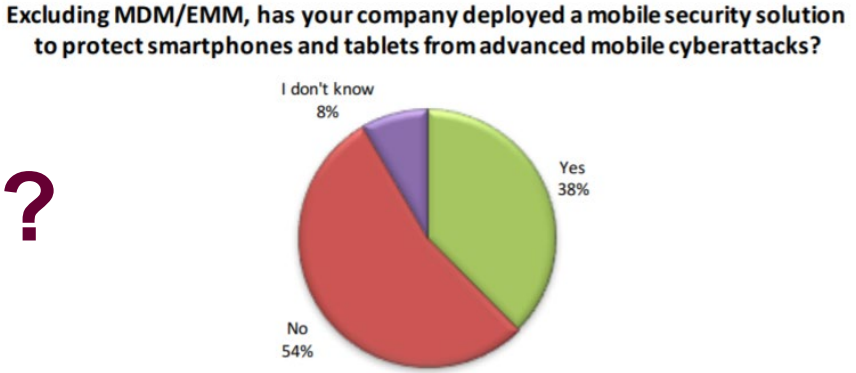
Algunos riesgos del BYOD

- Información sensible para la empresa puede ser divulgada al encontrarse en dispositivos robados, perdidos o en posesión de desempleados.
- Un dispositivo personal infectado puede conectarse a un red corporativa y comprometerla.
- Un usuario podría accidentalmente introducir un malware en la empresa a través de alguna app maliciosa que se hubiera descargado.
- El robo de información se podría realizar mediante carga de datos a un dispositivo personal.
- En general, es difícil implementar políticas de BYOD realmente efectivas, pues las fronteras entre lo personal y lo laboral son cada vez más difíciles de definir

¿Coste de una brecha de seguridad?



Mobile Device Management / Enterprise Mobile Management



¿Cómo se combate?

BYOD

Samsung Knox

- Crea dos contenedores de aplicaciones dentro de un mismo dispositivo
- Las apps de un contenedor no pueden comunicarse con las del otro
- Muy restrictivo, pero seguro

https://www.samsung.com/es/business

Android for Work

- Permite la instalación de un conjunto de apps que se utilizan exclusivamente para el entrono laboral y están aisladas del resto del dispositivo
- Limitado a las aplicaciones premium de Google Play

https://www.android.com/enterprise

Mobile Device Management

- Limita las acciones y permite instalar configuraciones automáticamente
- Si el dispositivo es del empleado, éste debe otorgar a la organización un gran control sobre él
- Muchas opciones disponibles (ver URL más abajo)

https://financesonline.com/mobile-device-management

Riesgos técnicos (OWASP Top 10 Mobile Risk)

- La Fundación OWASP (Open Web Application Security Project) es una comunidad dedicada a permitir la creación, desarrollo, adquisición, operación y mantenimiento de aplicaciones confiables y seguras

OWASP *Top Ten*: resumen de 10 vulnerabilidades más críticas en el desarrollo de *software*.

→

OWASP *Testing Guide*: Guía de mejores prácticas para test de intrusión.

→

OWASP *Development Guide*: Guía de programación segura.

- Riesgos de naturaleza técnica
  https://owasp.org/www-project-mobile-top-10
  - M1: Improper Platform Usage
  - M2: Insecure Data Storage
  - M3: Insecure Communication
  - M4: Insecure Authentication
  - M5: Insufficient Cryptography
  - M6: Insecure Authorization
  - M7: Client Code Quality
  - M8: Code Tampering
  - M9: Reverse Engineering
  - M10: Extraneous Functionality

M1 - Uso inapropiado
(ámbito)

- Se incluyen tanto los malos usos de la plataforma móvil como de sus controles de seguridad
- Incluye, aunque no se limita, al mal uso de
  - Intents en Android
  - Permisos
  - TouchID
  - KeyChain (relación de claves privadas y certificados en el almancén de credenciales)
  - Controles de seguridad que ofrezca el operativo
- En general este mal uso puede conllevar una llamada a un servicio existente en el backend debido a un control débil de las entradas en el mismo

M1 - Uso inapropiado
(Ejemplos)

- Una app Android solicita demasiados permisos, o los permisos incorrectos
- Una app iOS almacena en un fichero local información de seguridad (claves de sesión, contraseñas, trazas de ejecución,etc.) en lugar de utilizar un Keychain que permite hacerlo de manera cifrada
- Recordemos que también entrarían en esta categoría los riesgos que el uso inapropiado de la plataforma pudiera inducir en el backend que utiliza

M1 - Uso inapropiado
(Ejemplos)

Inyección SQL: inyección de comandos SQL no autorizados en una base de datos

XSS (*Cross Site Scripting*): carga de código JavaScript no autorizado

Falta de control de acceso: puede permitir al usuario acceder a partes no autorizadas de la aplicación, incluyendo cuentas de otros usuarios.

Errores en el manejo de sesión: puede permitir acceder a usuarios con sesiones antiguas que deberían estar cerradas.

M1 - Uso inapropiado

Atacantes	Vectores de Ataque	Vulnerabilidades de seguridad		Impacto técnico
Específico de cada App	Acceso fácil	Prevalencia común	Detección media	Impacto severo
Cualquier agente que pueda generar datos de entrada no confiables (incorrectos o no previstos) para la aplicación: un usuario, *malware*, una aplicación vulnerable, etc. con un objetivo malicioso	Son servicios a los que se puede acceder de forma remota y que, en la mayoría de las ocasiones, solo necesitan un registro previo con datos que pueden ser ficticios.	Para explotar esta vulnerabilidad, la organización debe ofertar un servicio web o llamada a un API que pueda ser consumida por la app. Esta app debe acceder a una API a través de un servicio web que sea vulnerable a cualquier vulnerabilidad de servidor (OWASP *Top Ten*). Entre ellas se encuentran la inyección SQL o el XSS.		El impacto es el de la vulnerabilidad del servidor aprovechada. En el peor caso, el impacto de una vulnerabilidad del servidor es severo. Una vulnerabilidad de inyección SQL puede llegar a exponer los datos de acceso de todos los usuarios e incluso permitir la administración completa del sitio.

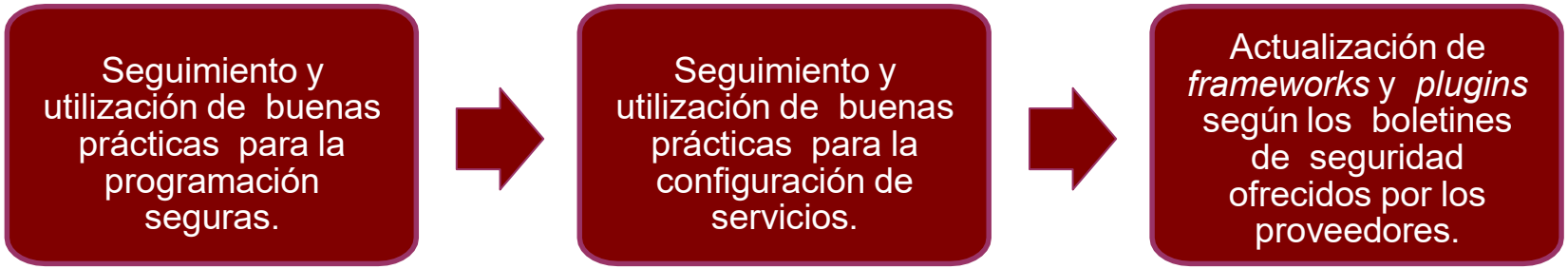
M1 - Uso inapropiado

(¿Soy vulnerable?)

- Probablemente **sí** si …
  - … Se violan los modelos de seguridad que cada plataforma define
    - IOS: https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf
    - Android: https://source.android.com/security
  - … Se introduce un error no intencionado, fruto de un error de programación, por ejemplo, a la hora de posicionar un flag o realizar una llama a un API la acción se implementará mal, o de un malentendido de cómo funcionan las protecciones existentes

M1 - Uso inapropiado
(Prevención)

- Uso de programación defensiva
- Asegurar una correcta configuración de la app
- Reduciremos la superficie del ataque si utilizamos servidores seguros, actualizados y verificados
- Este riesgo entra en íntima relación con el OWASP Cloud Top 10 (nube) y el OWASP Top 10 (web)



M2 – Almacenamiento inseguro

(ámbito)

- Hace referencia tanto
  - Al uso de medios de almacenamiento inseguro
  - Como a la fuga no intencionada de información que pudiera derivarse del incorrecto uso de los mismos
- Por ejemplo
  - Almacenamiento de credenciales y contraseñas en claro en ficheros de configuración.
  - Codificación de contraseñas de forma estática en el código de la aplicación.
  - No borrado de datos no necesarios para la aplicación.
  - Utilización de librerías criptográficas débiles.

M3 – Comunicaciones inseguras

(ámbito)

- Incluye, aunque no se limita, al uso de
  - Protocolos de registro poco robustos frente a ataques
  - Versiones no apropiadas de TSL y SSL
  - Protocolos débiles de negociación de sesión
  - Comunicación no cifrada de activos sensibles
- En definitiva, aquello que proporciona una protección en el transporte de datos insuficiente
  - Falta de comprobaciones de certificados
  - Negociación de parámetros débiles
  - Uso de librerías de terceros no confiables

M4 – Autenticación insegura

- Se incluyen tanto la autenticación del usuario como la gestión de sesiones
  - Fallar en la identificación del usuario o dispositivo, cuando ésta debería haberse realizado
  - No almacenar la identidad del usuario/dispositivo cuando ésta debería ser guardada
  - Usar métodos débiles de gestión de las sesiones

M5- Criptografía insuficiente

- Se utiliza criptografía, pero ésta no es lo suficientemente robusta para el activo que se desea proteger
- ¡Cuidado!
  - Si hablamos de TLS o SSL estamos en M3
  - Si la app no cifra la información almacenada estaremos en M2
- Se centra en el tipo de cifrado utilizado por parte de las apps (decisión de diseño)

M6 – Autorización insegura

- Esta categoría captura cualquier situación en la que no se verifica la autorización (credenciales) de acceso a un recurso
- ¡Ojo! Si no se autentica un usuario donde se debiera y se obtiene acceso anónimo a un recurso hablamos de un riesgo de tipo M4 (autenticación) y no de tipo M6 (autorización)
  - La autenticación es el proceso por el cual se identifica un cliente (persona) como válida para posteriormente acceder a ciertos recursos definidos
  - La autorización es el proceso sobre el cual se establecen que tipos de recursos están permitidos o denegados para cierto usuario o grupo de usuarios concreto

M7 – Calidad del código del cliente

- Aglutina todas las situaciones que tienen que ver con las decisiones tomadas en base a entradas poco o nada fiables y sus consecuencias
  - Vulnerabilidades de desbordamiento de buffer o de formato de string
  - Errores de implementación de código, que se corrigen reescribiéndolo adecuadamente
  - …

M8 – Manipulación de código

- Hace referencia al parcheo de código binario, modificación de recursos locales, o asignación dinámica de memoria,o al uso de métodos Hooking/Swizzling
- Con estas manipulaciones el objetivo del atacante es modificar el comportamiento del código para obtener un beneficio personal o monetario

M9 – Ingeniería inversa

- Análisis (estático o dinámico) del código fuente, librerías, algoritmos u otros activos de la app.
- El objetivo es obtener un conocimiento profundo de la app para
  - Descubrir y explotar nuevas vulnerabilidades (puede que aún desconocidas)
  - Revelar información sobre los servidores del back end utilizado, el tipo de criptografía utilizada (constantes, cifras, métodos), así como violar la propiedad intelectual de la app analizada

M10 – Funcionamiento extraño

- Los desarrolladores pueden incluir puertas traseras para activar funcionalidades o controles de seguridad adicionales que no deberían ser incluidos en la versión final (de producción) de la app
- Por ejemplo: deshabilitar la autenticación a dos niveles durante el test, o incluir la contraseña como un comentario en el código

Otras fuentes de información

- Common Vulnerabilities and Exposures list (CVE)
  - https://cve.mitre.org
- Common Weaknesses Enumeration (CWE)
  - https://cwe.mitre.org
- INCIBE (Instituto Nacional de CIBERseguridad)
  - Es una CNA (CVE Numbering Authority)
  - https://www.incibe-cert.es/alerta-temprana/vulnerabilidades
    - Ejemplo: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2018-8755
      - **Fabricante**: Nucom
      - **Modelo**: WR644GACV
      - **Vulnerable Software Version**: <= STA005
      - **Current Software Version**: STA006
      - **Tipo de Vulnerabilidad**: Authentication / Authorization Bypass
      - **CVSS Vector**: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
      - **CVE**: 2018-8755

Contenido

- Concepto de dispositivo móvil
- Fuentes de inseguridad: riesgos y vulnerabilidades en el ámbito móvil
- **Situación actual**

Y a pesar de conocer los riesgos, la situación es MUY preocupante

1 dispositivo móvil **robado** cada **53** segundos
- **70 millones** cada año
- Sólo un **7% se recuperan**

En 2017, el incremento de variantes de malware fue del **54%**

70% del SPAM móvil es fraudulento

96% de crecimiento en infecciones ocasionadas por malware en 2017

350% será el crecimiento de los puntos de acceso WiFi en 2019, lo que proporciona más oportunidades para ataques del tipo "man-in-the middle"

90 Billion de apps Android descargadas a finales de 2016 – más del **90%** de ellas afectadas por un problema de seguridad

Source: Evans Data Mobile Developer Survey Mobile Development Report
Source: Business Insider

Situación del mercado de apps

Google retira 13 juegos Android que contenían programas maliciosos

La mayoría de aplicaciones eliminadas eran simuladores de conducción que incluían publicidad sin permiso

JOSÉ MENDIOLA ZURIARRAIN
27 NOV 2018 - 14:12 CET

Aplicaciones de Android eliminadas por Google por contener programas maliciosos y denunciadas por analista de ESET Lukas Stefank

https://elpais.com/tecnologia/2018/11/26/actualidad/1543254783_206207.html

Lukas Stefanko
@LukasStefanko

Don't install these apps from Google Play - it's malware.

Details:
-13 apps
-all together 560,000+ installs
-after launch, hide itself icon
-downloads additional APK and makes user install it (unavailable now)
-2 apps are #Trending
-no legitimate functionality
-reported

♡ 1.445 14:17 - 19 nov. 2018

1.601 personas están hablando de esto

- Y esto a pesar de la existencia del servicio Google Play Protect
  https://www.android.com/intl/es_es/play-protect

Este grave problema de seguridad no fue detectado por los propios protocolos de Google que filtran el contenido en Google Play, sino que fue desvelado por el analista de ESET Lukas Stefanko quien, mediante un mensaje en su perfil de Twitter, desveló que 13 aplicaciones que acumulaban más de 560.000 descargas estaban infectadas con *malware*. El críptico mensaje de este analista explica que las mencionadas aplicaciones, que ya han sido retiradas por Google de la tienda, instalaban un archivo APK adicional no relacionado con el objetivo del juego y sin una "función legítima".

Incluso en ámbitos críticos

ANDY GREENBERG SECURITY 09.10.18 01:00 PM

HACKERS CAN STEAL A TESLA MODEL S IN SECONDS BY CLONING ITS KEY FOB

First, they use the Proxmark radio to pick up the radio ID of a target Tesla's locking system, which the car broadcasts at all times. Then the hacker swipes that radio within about 3 feet of a victim's key fob, using the car's ID to spoof a "challenge" to the fob. They do this twice in rapid succession, tricking the key fob into answering with response codes that the researchers then record. They can then run that pair of codes through their hard drive's table to find the underlying secret key—which lets them spoof a radio signal that unlocks the car, then starts the engine.

The KU Leuven researchers say they told Tesla about their findings in August 2017. Tesla acknowledged their research, thanked them, and paid them a $10,000 "bug bounty" for their work, the researchers say, but it didn't fix the encryption issue until its June encryption upgrade and more recent PIN code addition.

https://www.wired.com/story/hackers-steal-tesla-model-s-seconds-key-fob

Versiones y precios del Tesla Model S

Versión	Combustible	Precio
Model S 75	Eléctrico	94.300 €
Model S 75D	Eléctrico	100.100 €
Model S 90D	Eléctrico	111.300 €
Model S P100D	Eléctrico	163.400 €

Robo de un Tesla

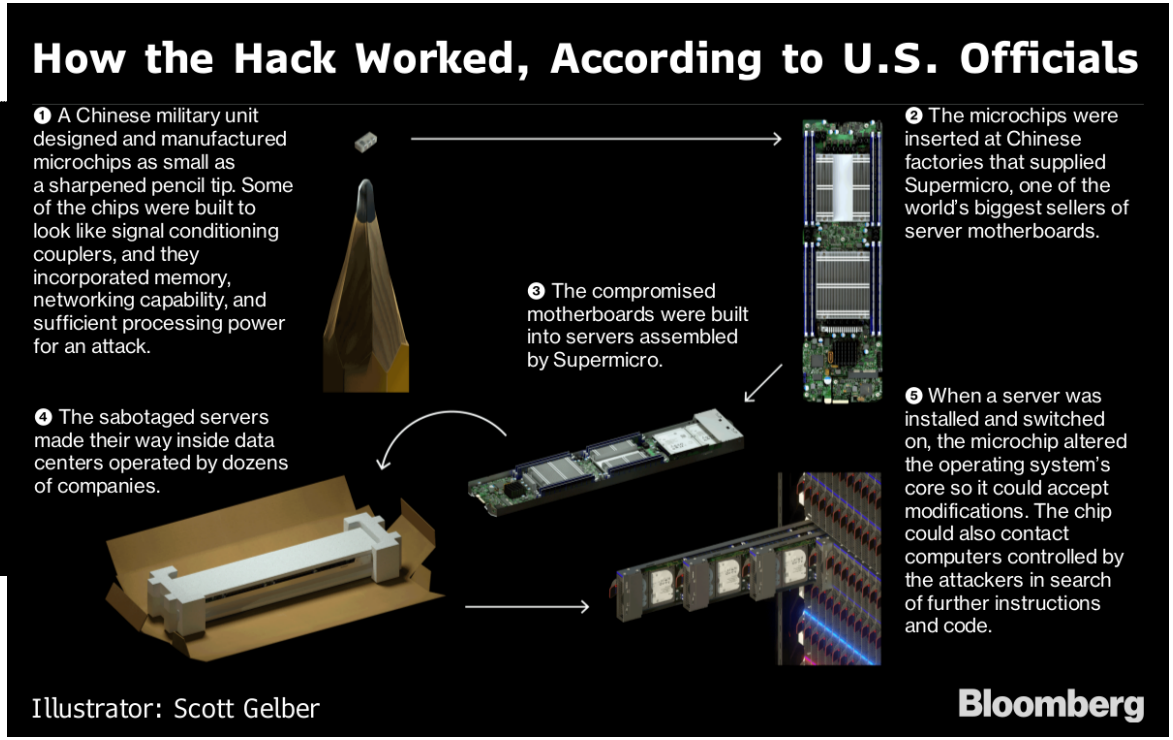
https://www.wired.com/story/hackers-steal-tesla-model-s-seconds-key-fob

Problemas hay a todos los niveles

- Se buscan dispositivos móviles cada vez más complejos, pequeños y autónomos → Problema de los troyanos en el HW

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.



https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

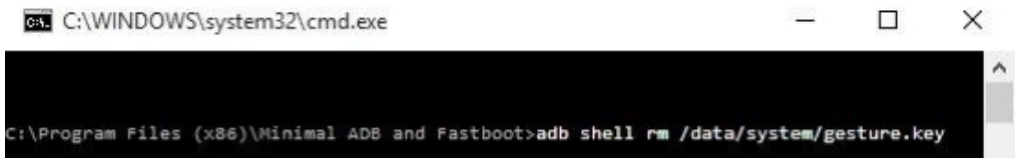
El eslabón más débil de la cadena

- No todo es una cuestión técnica, la concienciación es también muy importante
  - Ejemplo de cómo la ingeniería social puede dar al traste con una solución de seguridad

https://www.youtube.com/watch?v=lc7scxvKQOo

Y muchas veces son (al menos un poco) culpa nuestra

- Deseamos coger los dispositivos y poderlos utilizar inmediatamente → se evita el uso de contraseñas robustas o PIN (40% de los usuarios lo hacen)
  - Desbloqueo por reconocimiento facial
    - Aunque los rangos son únicos, pueden reproducirse con impresión 3D: https://andro4all.com/2018/12/android-seguridad-cara-3d
  - Uso de patrón de desbloqueo del móvil
    - Borrar el patrón de desbloqueo (sólo funciona si la depuración por USB fue activada en el dispositivo)



    - Ataques térmicos: https://www.youtube.com/watch?v=a2Q64XmZpc4

Conclusión

- Gran potencial y evolución de la computación móvil en los últimos años
- Asistimos a la aparición de nuevos dispositivos y servicios con potencial para cambiar nuestro día a día (tanto a nivel laboral como doméstico)
- La seguridad de estos dispositivos móviles, sus comunicaciones y las apps que ejecutan es todo un reto
  - Necesitamos mejorar nuestra “higiene digital”
  - Los dispositivos Android son los más vulnerables y atacados
  - ¿Y cuales son los riesgos y amenazas que afectan a estos dispositivos móviles? ¡¡¡ Vamos a verlo en el próximo tema !!!