

Mobile Hacking layer

Layer 1

تحليل علم هجمات اختراق المحمول - الجهاز

<p>التطبيقات</p> <p>الوصول والرسائل SMS</p> <p>المتصفحات</p>	<p>Escalated Privilege</p> <p>No Encryption / Weak encryption</p> <p>Improper SSL validation</p> <p>Sensitive Data Storage</p> <p>Config Manipulation</p> <p>Dynamic Runtime Injection</p> <p>Access to device / user info</p> <p>unintended permissions</p>	<p>SMishing</p> <p>Baseband Attacks</p> <p>Phishing</p> <p>Framing</p> <p>ClickJacking</p> <p>Buffer overflow</p> <p>Man-in-the-mobile</p> <p>Data Caching</p>	<p>الطرق المحتملة للاختراق</p>
--	--	--	--------------------------------

Layer 2

تحليل علم هجمات اختراق المحمول - الشبكة

<p>شبكة الاتصال</p> <p>شبكة الإنترنت (WiFi) - تشفير ضعيف أو بلا تشفير</p> <p>جهاز الاتصال بالإنترنت غير موثوق</p> <p>على زخم الاتصال بالإنترنت sniffing</p> <p>Man-in-the-middle (MITM)</p> <p>session Hijacking</p> <p>DNS poisoning</p> <p>SSLstrip</p> <p>Fake SSL Certificate</p>	<p>الطرق المحتملة للاختراق</p>
---	--------------------------------

layer 3

تحليل علم هجمات اختراق المحمول - مركز البيانات

<p>قواعد البيانات</p> <p>SQL Injection</p> <p>Privilege Escalation</p> <p>Data Dumping</p> <p>OS Command Execution</p>	<p>قواعد الإنترنت</p> <p>لغات النص</p> <p>عدم التعرف على القوائم</p> <p>Cross-site Scripting (XSS)</p> <p>Cross-site Request Forgery</p> <p>ضرب في التحقق من المصادقات</p> <p>Brute Force Attacks</p>	<p>الطرق المحتملة للاختراق</p>
--	---	--------------------------------

Overview



مخاطر و ثغرات منصات الجوال



مشاكل أمنية لمتاجر التطبيقات



Download on the **App Store** | **Google play**



فحص وتوقيع التطبيق قبل النشر غير دقيق وقد تسرب بعض التطبيقات الوهمية الخبيثة.

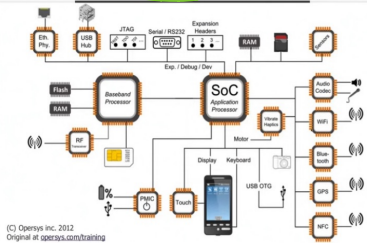
متاجر التطبيقات هدف للمخترقين لنشر التطبيقات الخبيثة فيهم.

المخترقون يستخدمون الهندسة الاجتماعية لجذب العملاء لتحصيل تطبيق من خارج متجر التطبيقات.

التطبيقات الخبيثة تؤثر سلباً على بيانات التطبيقات الأخرى وترسل بيانات العملاء الحساسة إلى المخترق بسهولة.



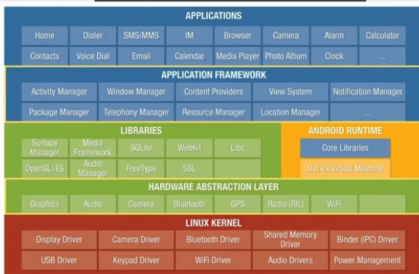
نظام الجوال



(C) Openix Inc. 2012
Original at openix.com/training



هيكل نظام الأندرويد



مشاكل Sandboxing في التطبيقات



مشاكل Sandboxing في التطبيقات



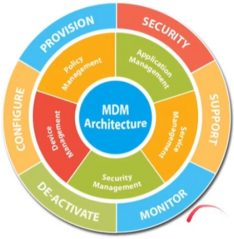
*for android pentest:

- Network spoofer (http)
- faceNiff (http)
- spy phone (source code)

*On window andriller

android data extractor like

* create a payload for android using ahmyth on github

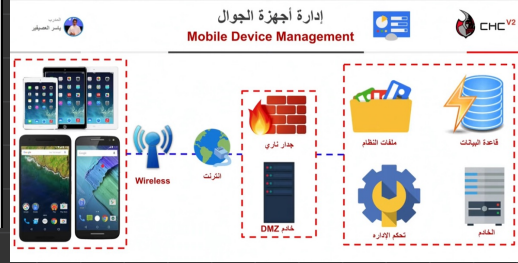


منصة إدارة التطبيقات والبيانات والإعدادات لكل أنواع الأجهزة الذكية مثل الجوال و التابلت والمحمول والحاسوب.

تساعد خدمة (إدارة أجهزة الجوال) على تنظيم التواصل بين الموظفين في الشركات والمؤسسات وتكفل تكلفة الإدارة وتحمي من خطر قلة الأمان.

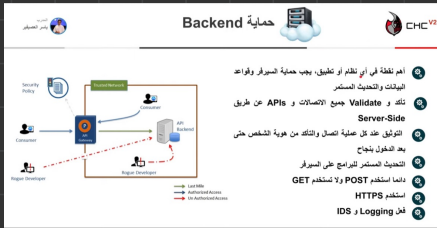
تساعد المدير لتنظيم التطبيقات في جميع أجهزة الجوال داخل معينة أو قسم من أقسام الشركة لمتابعة ومراقبة ودعم الموظفين عبر الجوال.

يمكن تنظيم استخدام الموظفين والإدارة معا داخل شركة معينة.



How to secure:

- x-ray app. for
- android-vts



حماية Backend

1. دعم نقطة في أي نظام أو تطبيق، يجب حماية مسارات وأقواس
2. البينات والتحديث المستمر
3. التتبع عند كل عملية الاتصال و APIs من طريق
4. Server-Side
5. التتبع عند كل عملية الاتصال و التتبع من عوية الشخص حتى
6. بعد القول بنجاح
7. التحديث المستمر التراجع على السيرفر
8. GET استخدم POST لا تستخدم
9. HTTPS استخدم
10. IDS Logging

حماية تطوير التطبيقات



- reverse engineering في الاختراق و
- الاختيار الأمني قبل طرح أي تطبيقات إلى المتاجر من قبل طرف ثالث
- الحذر من استخدام خدمات الطرف الثالث مثل
- Analytic or crash services
- التتبع من ان الجوال Jailbreak/Root detection
- تشفير الملفات Obsufation في الأيفون و Livn و الأندرويد و
- Proguard
- Decguard
- استخدام Anti-Debugger code
- لاتحزن اي بيانات أنت لست بحاجة اليها!
- لا تترك بالمستخدم أبدا

- use private vpn
- use multi-factor
- use last pass

تأمين وحماية الجوال



	عدم عمل Rooting and JailBreaking		حدث نظام التشغيل والتطبيقات باستمرار	
	فعل خاصية مسح البيانات في حالة الدخول المتكرر الخاطئ		تحميل التطبيقات من المتجر الرئيسي	
	ضع وقت محدد لإغلاق الشاشة تلقائيا في حالة عدم الإستخدام		استخدم كلمة مرور قوية و تثبيت تطبيقات حماية و مضاد فيروسات	