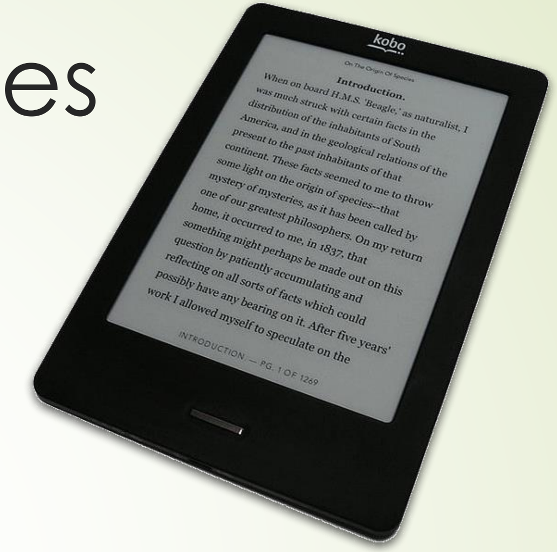
Mobile Device Security

By: Andrei Martinenco, Noor Ahmed, Max Averbach

Popular mobile devices



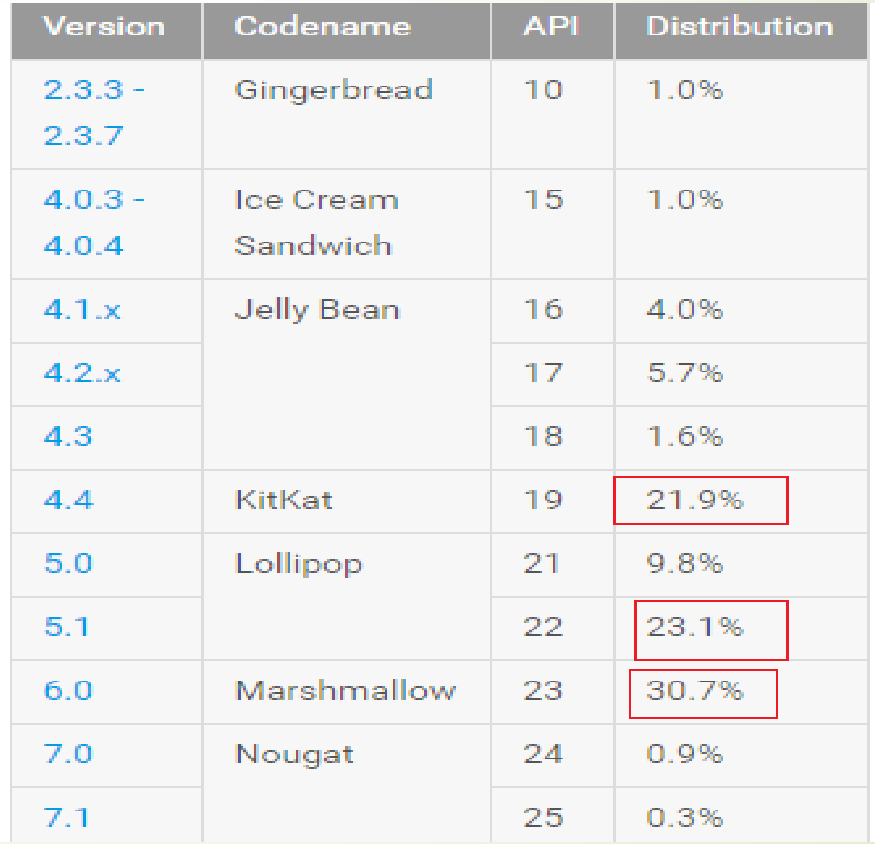
Introduction.

When on board H.M.S. 'Beagle,' as naturalist, I was much struck with certain facts in the distribution of the inhabitants of South America, and in the geological relations of the present to the past inhabitants of that continent. These facts seemed to me to throw some light on the origin of species--that mystery of mysteries, as it has been called by one of our greatest philosophers. On my return home, it occurred to me, in 1837, that something might perhaps be made out on this question by patiently accumulating and reflecting on all sorts of facts which could possibly have any bearing on it. After five years' work I allowed myself to speculate on the

- Smartphones
  - iPhone, Android
- Tablets
  - iPads, Samsung Galaxy Tab, Sony Xperia Z4, etc
- E-book reader
  - Amazon Kindle, Kobo
- Smartwatches
  - Apple watch, Samsung gear

Android Security

- Android security is good but the OS version and device diversity makes security hard to perfect



Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	1.0%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	1.0%
4.1.x	Jelly Bean	16	4.0%
4.2.x		17	5.7%
4.3		18	1.6%
4.4	KitKat	19	21.9%
5.0	Lollipop	21	9.8%
5.1		22	23.1%
6.0	Marshmallow	23	30.7%
7.0	Nougat	24	0.9%
7.1		25	0.3%

Ragentek Group

- Chinese company developed the firmware
- Left 3 million devices vulnerable
- Firmware:
  - Does not encrypt the communication sent and received to the phone
  - Does not rely on code-signing to authenticate legitimate apps

- US was #1 affected country
- BLU phones were affected

Qualcomm chipset

- 900 Million Qualcomm devices were exposed to vulnerability called QuadRooter
- Discovered by security company “Check Point” in 2016
- Allows hackers to gain root access to your phone.
    - Collect stored data
    - Key log
    - Control the camera
    - Track GPS location
- Attacker exploits these vulnerabilities using a malicious app. (No permissions required)

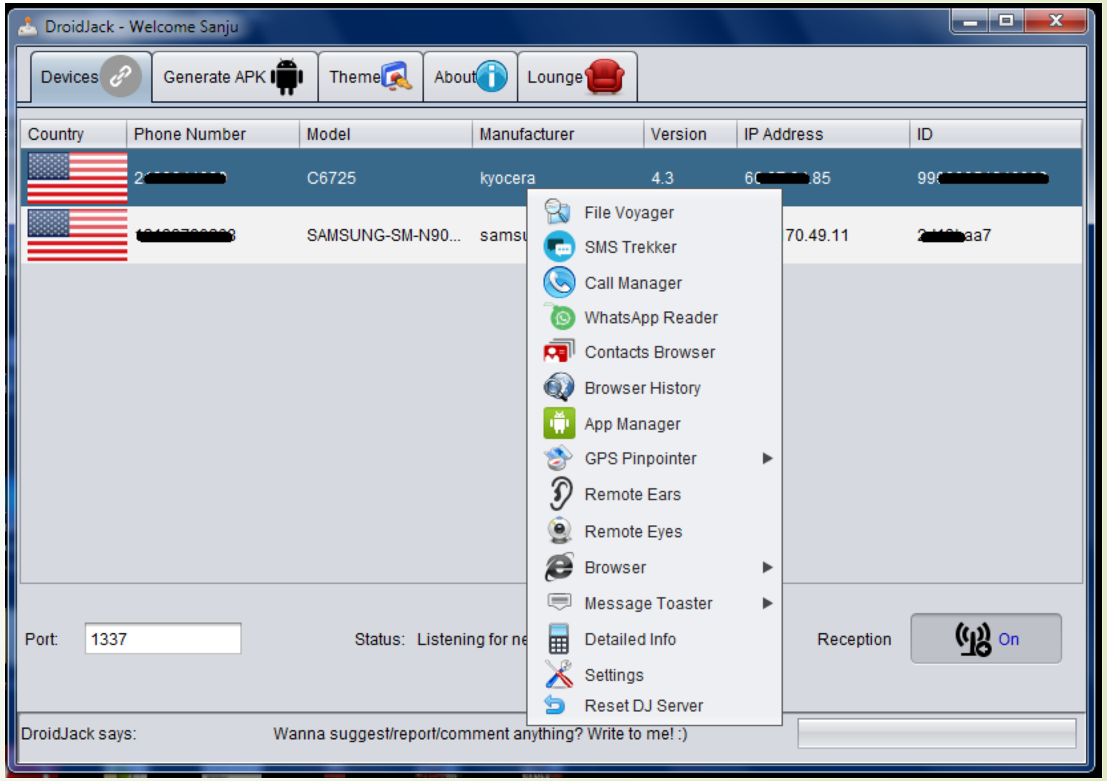
How to protect?

- QuadRoot Scanner by “Check Point Labs”
- Download only trusted apps from trusted sources (Google Play)
- Keep your device up to date
- Avoid side loading (.APK) files from untrusted sources (Pokémon GO)
- Watch out for suspicious permissions (Flashlight)
- Use your phone on trusted wifi networks
- Use Anitvirus protection
- Samsung devices are not in danger (Exynos)

Dangers of side loading

- Malicious Pokémon GO app with “DroidJack” malware.
- Gives full control over victims phone

- Control Wifi
- Control GPS
- Take pictures
- Record video
- Download/Upload files
- Many more



Country	Phone Number	Model	Manufacturer	Version	IP Address	ID
🇺🇸	2[redacted]	C6725	kyocera	4.3	6[redacted].85	99[redacted]
🇺🇸	[redacted]3	SAMSUNG-SM-N90...	samsu		70.49.11	2[redacted]aa7

Port: 1337

Status: Listening for ne

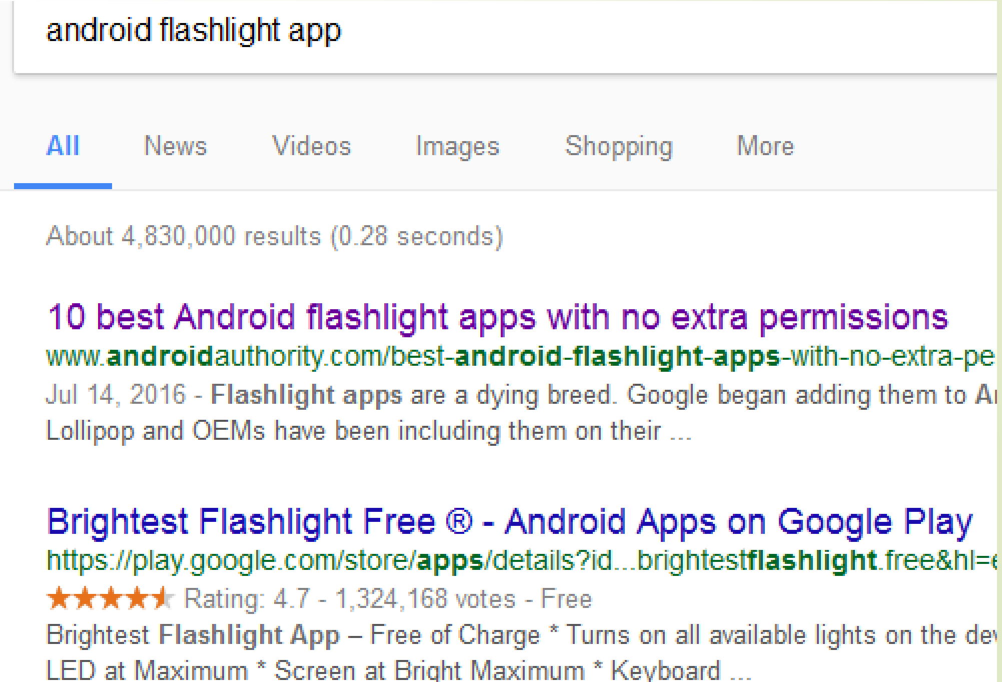
Reception On

DroidJack says: Wanna suggest/report/comment anything? Write to me! :)

Permissions

- “Brightest Flashlight Free” was installed on 50 - 100 million devices.
- This app was sharing GPS location and unique device identifier to the third party advertisers without user’s consent
- The app presented users with an option not to share any information, even thought it already did.
- Developer settles with FTC

Federal Trade Commission



android flashlight app

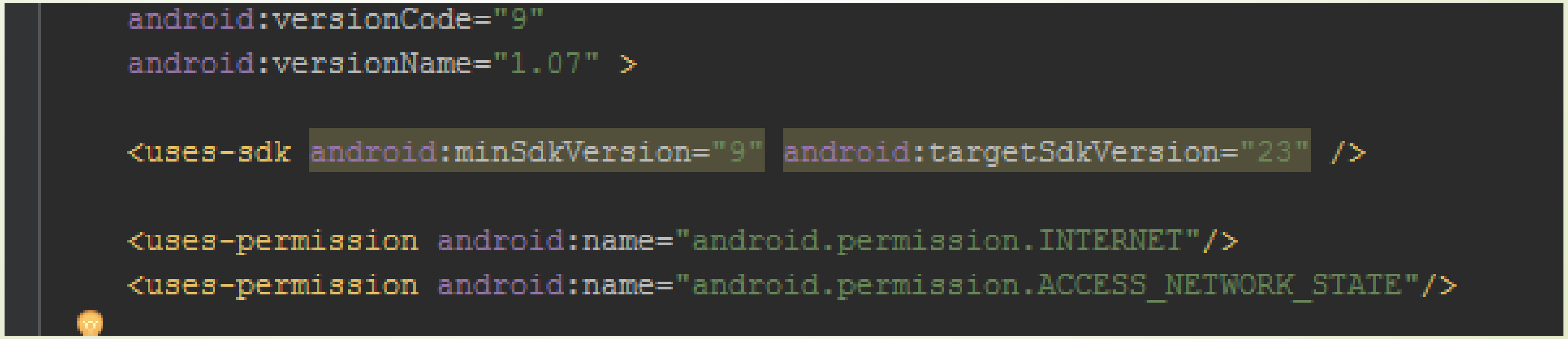
About 4,830,000 results (0.28 seconds)

10 best Android flashlight apps with no extra permissions
www.androidauthority.com/best-android-flashlight-apps-with-no-extra-pe
Jul 14, 2016 - Flashlight apps are a dying breed. Google began adding them to A
Lollipop and OEMs have been including them on their ...

Brightest Flashlight Free ® - Android Apps on Google Play
https://play.google.com/store/apps/details?id...brightestflashlight.free&hl=
★★★★★ Rating: 4.7 - 1,324,168 votes - Free
Brightest Flashlight App – Free of Charge * Turns on all available lights on the de
LED at Maximum * Screen at Bright Maximum * Keyboard ...

Changes to Permissions

- Android 6.0 (API Level 23) introduced new permission system
- System permissions are divided into two categories:
  - Normal permissions (do not risk user's privacy)
  - Dangerous permissions – give access to the user's confidential data. User has an option to grant that permission.
- The app has to target API level 23.



```
    android:versionCode="9"
    android:versionName="1.07" >

    <uses-sdk android:minSdkVersion="9" android:targetSdkVersion="23" />

    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
```

Apple Mobile Device Security

Apple Mobile Device Security

- When Apple refused to unlock an iPhone 5C for the FBI, the conversation around its encryption practices moved center stage.
- Apple's iOS devices are known for their strong security, partly because Apple controls the entire device ecosystem -- hardware, firmware, and software.

Apple Mobile Device Security

- Recently, at Apple's 2016 WWDC event, the company announced that it would require the use of its App Transport Security (ATS) feature in all apps by January 1, 2017. This would essentially force all app traffic to run through encrypted HTTPS connections from now on.

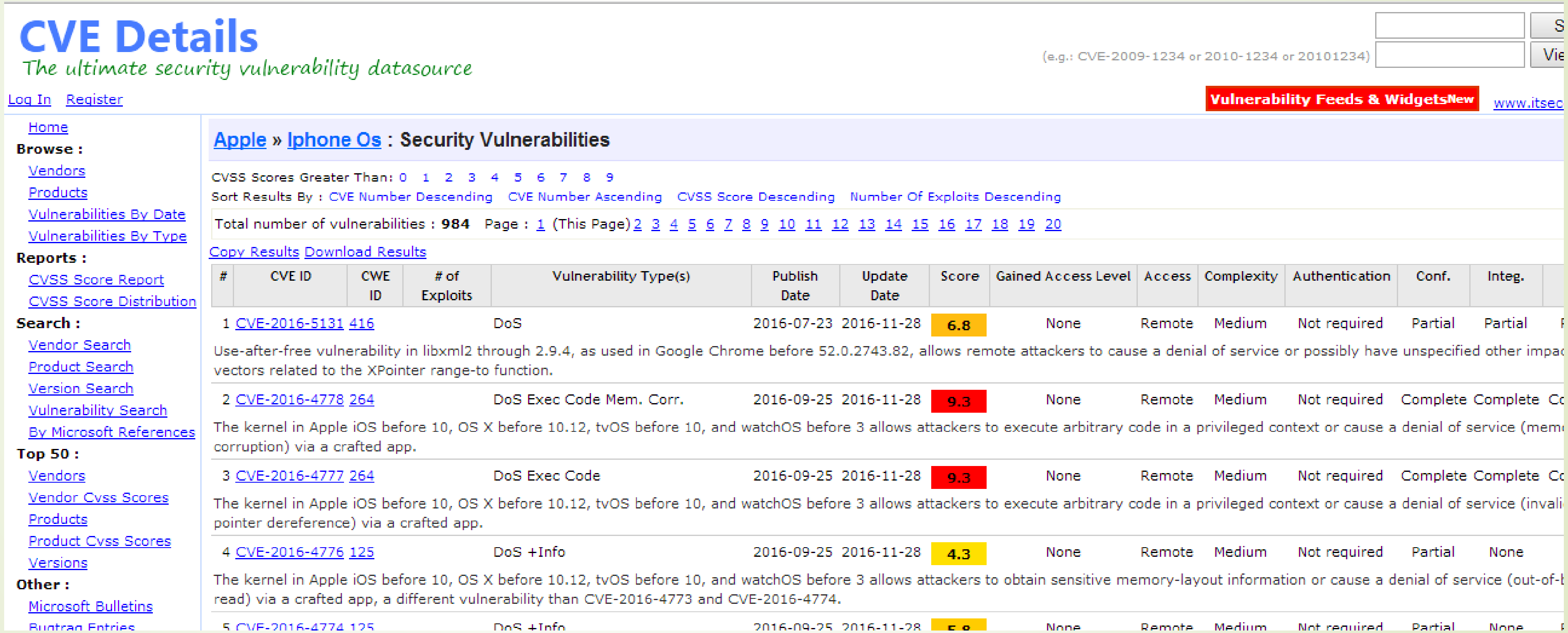
Apple Mobile Device Security

- In order to develop and install apps on iOS devices, developers must register with Apple and join the Apple Developer Program.
- The real-world identity of each developer, whether an individual or a business, is verified by Apple before their certificate is issued.

Apple Mobile Device Security

- Once an app is verified to be from an approved source, iOS enforces security measures designed to prevent it from compromising other apps or the rest of the system.

iPhone Vulnerabilities



CVE Details
The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register

Vulnerability Feeds & WidgetsNew www.itsec

Home
Browse :
- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :
- CVSS Score Report
- CVSS Score Distribution

Search :
- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft References

Top 50 :
- Vendors
- Vendor Cvss Scores
- Products
- Product Cvss Scores
- Versions

Other :
- Microsoft Bulletins
- Bugtraq Entries

Apple » Iphone Os : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **984** Page : 1 (This Page) 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	
1	CVE-2016-5131	416		DoS	2016-07-23	2016-11-28	6.8	None	Remote	Medium	Not required	Partial	Partial	P
Use-after-free vulnerability in libxml2 through 2.9.4, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have unspecified other impac vectors related to the XPointer range-to function.														
2	CVE-2016-4778	264		DoS Exec Code Mem. Corr.	2016-09-25	2016-11-28	9.3	None	Remote	Medium	Not required	Complete	Complete	Co
The kernel in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (mem corruption) via a crafted app.														
3	CVE-2016-4777	264		DoS Exec Code	2016-09-25	2016-11-28	9.3	None	Remote	Medium	Not required	Complete	Complete	Co
The kernel in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (invali pointer dereference) via a crafted app.														
4	CVE-2016-4776	125		DoS +Info	2016-09-25	2016-11-28	4.3	None	Remote	Medium	Not required	Partial	None	
The kernel in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows attackers to obtain sensitive memory-layout information or cause a denial of service (out-of-l read) via a crafted app, a different vulnerability than CVE-2016-4773 and CVE-2016-4774.														
5	CVE-2016-4774	125		DoS +Info	2016-09-25	2016-11-28	5.8	None	Remote	Medium	Not required	Partial	None	P

Trident Flaw

- In August 2016, Apple released a new security update which fixes the spying flaw, aka Trident Flaw.
- the spy can gain access to the device's kernel – the core of the operating system – which has privileged access to operate the phone. This means it can turn on the camera or microphone, install surveillance software, and read the contents of emails and messaging apps, as well as calendars.
- All of this can happen without the user knowing as it occurs in the phone's underlying code.

Trident Flaw

- For a phone to be breached, all that has to happen is for the user to click a link that opens in Safari, which activates a piece of spying software named "Pegasus".

Exodus Intelligence

- Apple offers 200k for zero-day (unknown at the time of release) new vulnerabilities in the iOS.
- Black Hat firm Exodus Intelligence offers 500k.
- Exodus then sells the known vulnerabilities on the Black Market.

Smart watches

- Apple watch
- Android watch

SMART WATCH IS A WEARABLE COMPUTERIZED WRISTWATCH, THEY RELY ON WIRELESSLY CONNECTED SMARTPHONE TO PERFORM MANY OF ITS DEFAULT FUNCTIONS, SUCH AS CALLING, TEXTING, ETC..

How secure is your smart watch?

Security Issues:

- Many companies who have tested smartwatches to know how secure they are, they found many serious security flaws in a smartwatch, such as:
  - Insufficient Authentication
  - Lack of Encryption
  - Privacy Problems

- In 2015 HP Fortify finds 100 percent of tested smartwatches exhibits security flaws.
- A 2015 study by Hewlett-Packard found that "100 percent" of popular smart watches were vulnerable to some form of security attack.

Security Issues

- Insufficient Authentication:
  - According to the Analysis report by HP Fortify:
    1. 30% of unit tested were vulnerable to account harvesting, that is attacker could gain access to the device and data due to the combination of weak password policy and lack of account lockout
    2. The smartwatches tested allows user to upload their information to a server on cloud, which then returns a subset of the user's contacts that are using the service

    A report from Trend Micro says the lack of passwords or other authentication methods makes smart watches uniquely vulnerable to hackers.

Security Issues

- Lack of Encryption:
  - According to the Analysis report by HP Fortify:

  100 percent of the test products implemented transport encryption using SSL/TLS, 40 percent of the cloud connections make use of weak security cyphers and are vulnerable to POODLE attacks due to their continued use of SSL v2.

- In 2015, researchers from University of New Haven, managed to pull emails, messages, contacts and complete health data from the Samsung Gear 2 and contact lists from LG G watch. This is because Samsung and LG do not properly encrypt data on their smart watches.

Lack of encryption leaves LG and Samsung smartwatch data open to hackers

Apple watch security issues

- Payment fraud using apple pay: (Verbal Explanation)
- Apple watch reset issue (Verbal explanation)

Questions:

1. What is the most common vulnerability for the iPhone?
2. What is the name of the feature that Apple required by January, 2017 in all of its apps?
3. What is the name of the program that a developer must register with in order to develop apps for the iPhone?
4. Because of insufficient authentication on smartwatch, what should we do to strengthen the authentication?
5. Which Android version introduced new permission system?

Answers

1. Dos
2. App Transport Security (ATS)
3. Apple Developer Program
4. Use two-factor Authentication. Available both on Android Watch(using google authenticator) and Apple watch.
5. 6.0

References:

- https://arstechnica.com/security/2016/11/powerful-backdoorrootkit-found-preinstalled-on-3-million-android-phones/
- http://www.zdnet.com/article/smartwatch-security-fails-to-impress-top-devices-vulnerable-to-cyberattack/
- https://www.wired.com/2016/08/quadroot-android-vulnerability-qualcomm/
- http://blog.checkpoint.com/2016/08/07/quadrooter/
- http://www.techradar.com/news/phone-and-communications/a-pokemon-go-malware-app-was-downloaded-by-half-a-million-people-1328655
- http://www.theverge.com/2013/12/6/5181472/brightest-flashlight-free-ftc-location-data-settlement
- https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived

References:

- http://www.zdnet.com/article/the-state-of-mobile-device-security-android-vs-ios/
- https://www.apple.com/business/docs/iOS_Security_Guide.pdf
- https://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-15556/Apple-Iphone-Os.html
- http://www.telegraph.co.uk/technology/2016/08/26/iphone-spying-scare-what-you-need-to-know-about-apples-critical/
- https://9to5mac.com/2016/08/10/iphone-hack-bounty-apple-exodus-intelligence/
- http://www.eetimes.com/author.asp?section_id=36&doc_id=1327588
- http://scienceline.org/2016/01/how-secure-is-your-smart-watch/
- http://blog.trendmicro.co.uk/security-flaws-common-on-most-popular-smartwatches/#more-363
- http://bgr.com/2015/05/20/apple-watch-security-flaw-apple-pay/
- http://www.dailymail.co.uk/sciencetech/article-3081478/Apple-Watch-security-flaw-leaves-vulnerable-thieves-Device-reset-paired-phone-minutes.html
- https://en.wikipedia.org/wiki/Smartwatch