Hacking Exposed 7
Network Security Secrets & Solutions

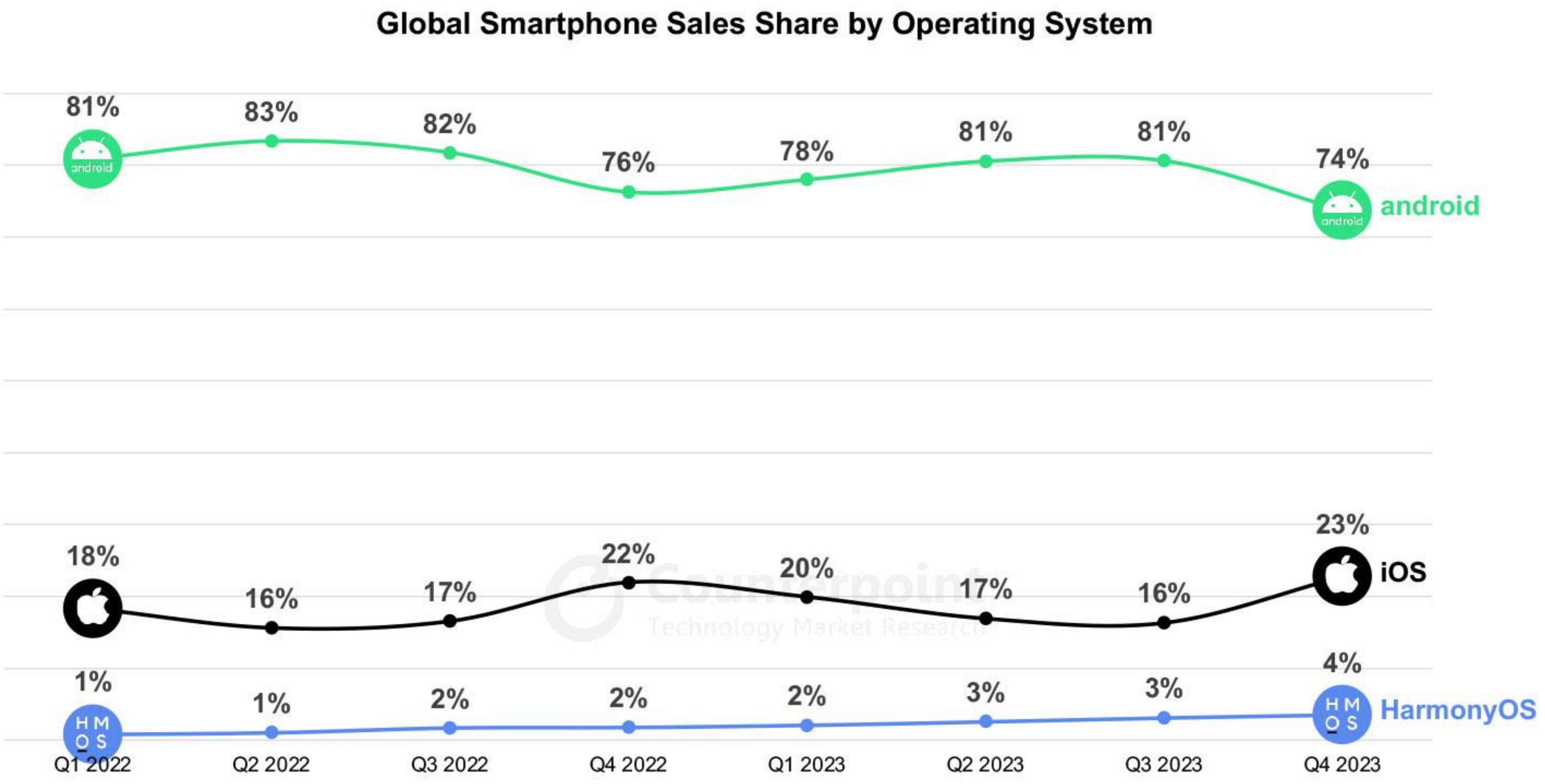
Chapter 11 Mobile Hacking

Outline

- Hacking Android
  - Android fundamentals
  - Hacking your Android
  - Hacking other’s Android
- Hacking iOS
  - How secure is iOS
  - Hacking your iOS
  - Hacking other’s iOS

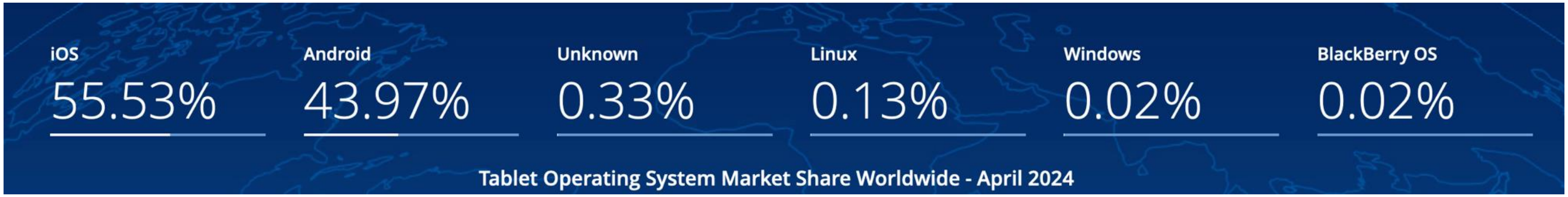
Hacking Android

OS Market Share: Smartphones



Source: https://www.counterpointresearch.com/insights/global-smartphone-os-market-share/#

OS Market Share: Tablets



iOS	Android	Unknown	Linux	Windows	BlackBerry OS
55.53%	43.97%	0.33%	0.13%	0.02%	0.02%

Tablet Operating System Market Share Worldwide - April 2024

Source: https://gs.statcounter.com/os-market-share/tablet/worldwide

Android's Position

- People argue about whether Android is truly open-source
  - Some products and versions are kept secret by Google

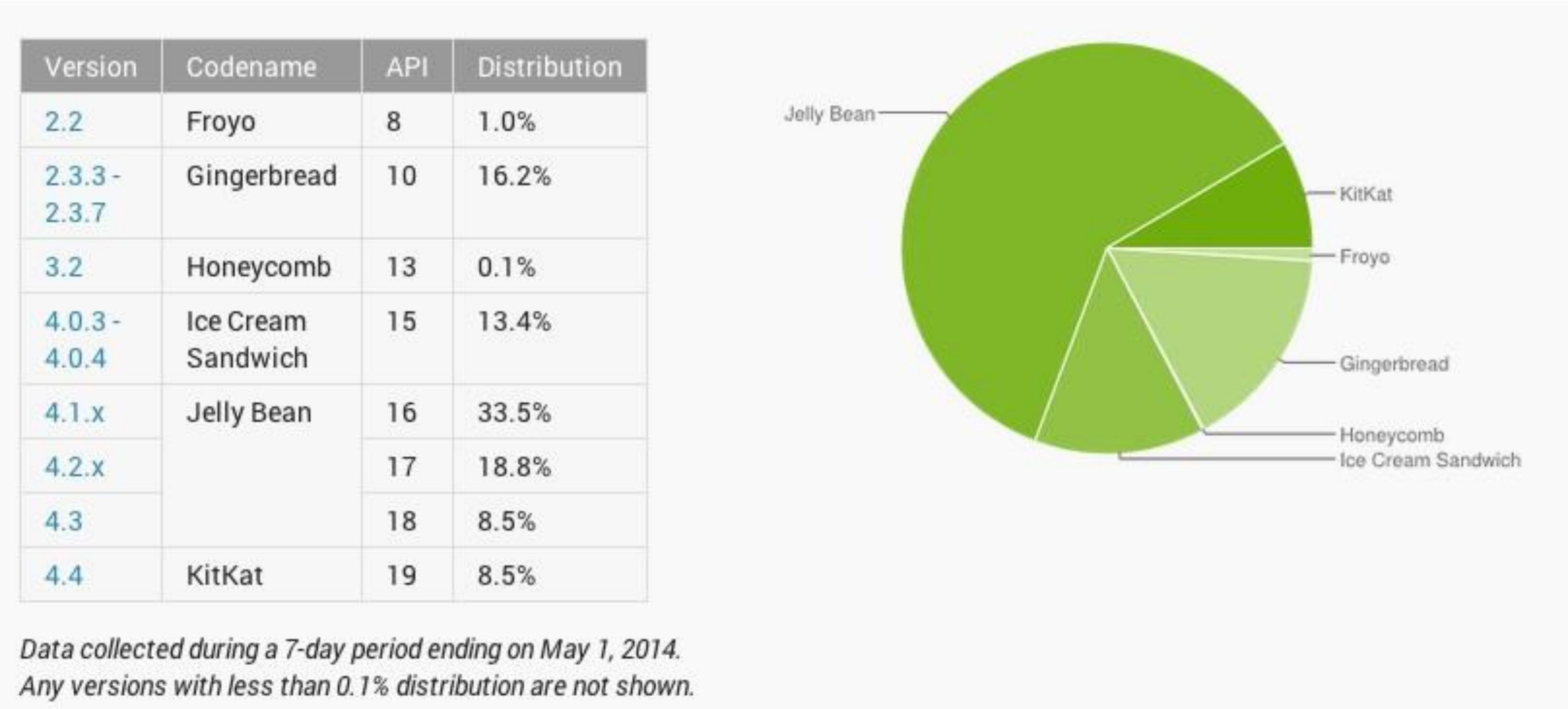
- Uses Linux kernel, developers can use C and C++

- Tools like Nmap and tcpdump can be installed

Fragmentation

- Many Android users are using out-of-date OS versions
  - Only 1.8% of Android devices were using the latest version on Oct 1, 2012
- As of May, 2014, 8.5% of devices were running the latest version
- As of of February 2024, **29%** of Android devices run the latest version (13)

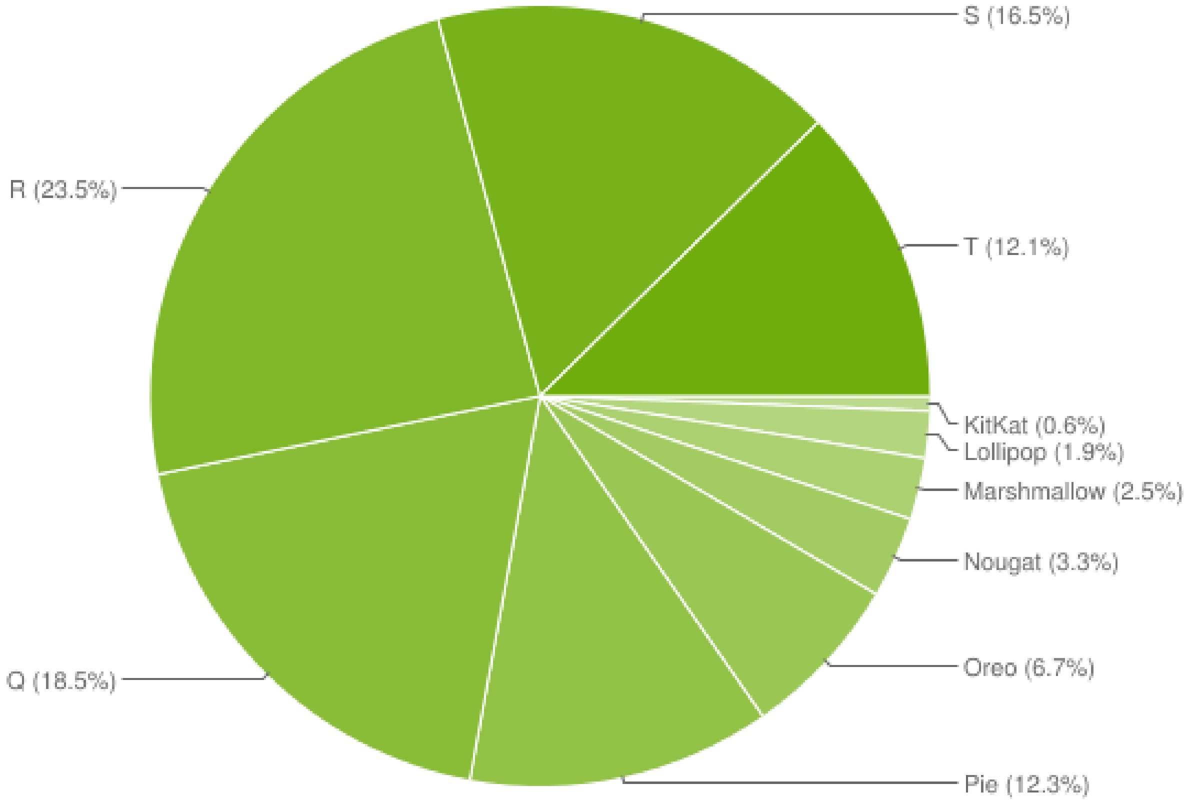
Android Version Popularity
2014 vs today



Version	Codename	API	Distribution
2.2	Froyo	8	1.0%
2.3.3 - 2.3.7	Gingerbread	10	16.2%
3.2	Honeycomb	13	0.1%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	13.4%
4.1.x	Jelly Bean	16	33.5%
4.2.x		17	18.8%
4.3		18	8.5%
4.4	KitKat	19	8.5%

Data collected during a 7-day period ending on May 1, 2014.
Any versions with less than 0.1% distribution are not shown.

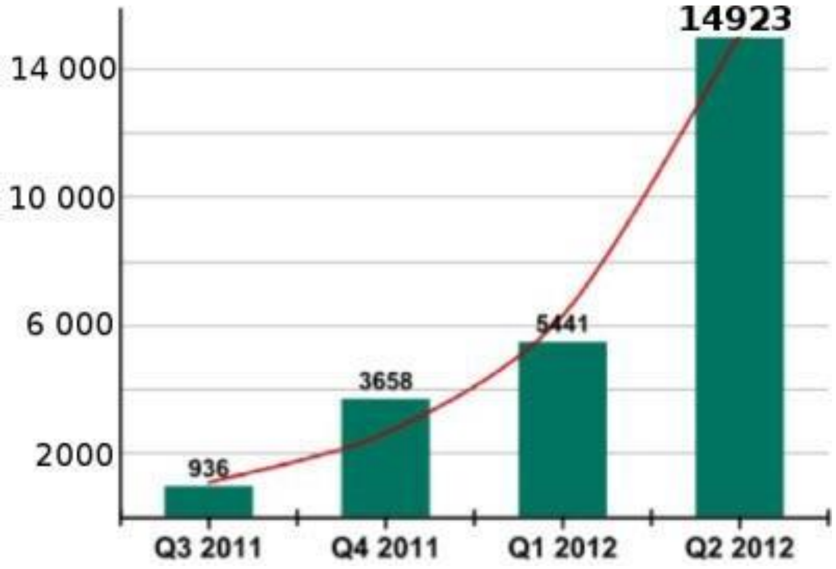
Android Version Popularity 2014 vs today



Source: https://9to5google.com/2023/04/13/android-13-market-share-stats/

Android Malware
2014 vs today

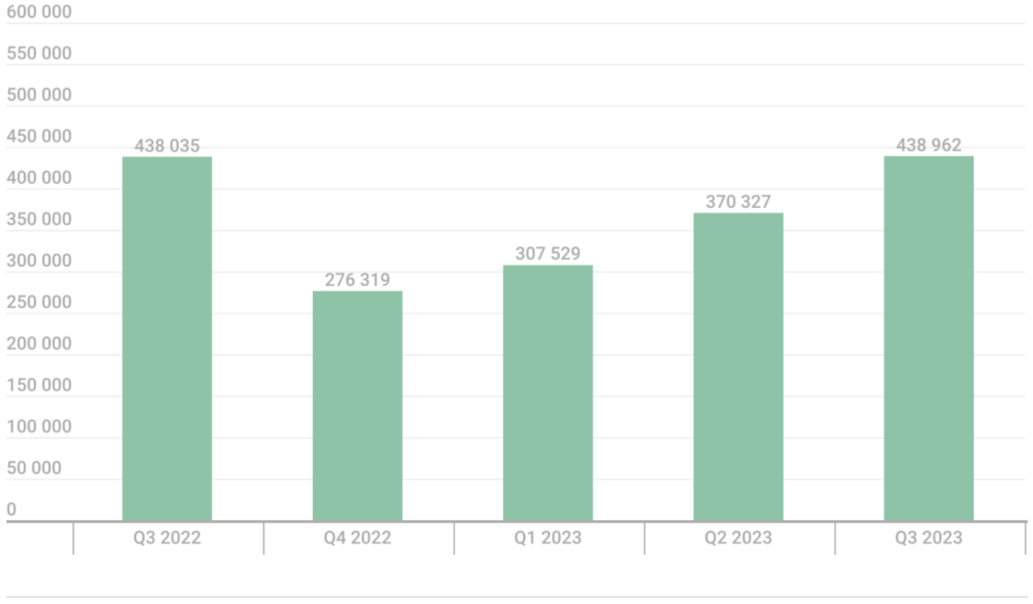
- Explosive growth
- You need antivirus on your Android
- Such as LookOut
- 10 million Android malware signatures in Jan. 2014



Detected malicious packages

Android Malware
2014 vs today

- 8 million *Mobile* malware signatures in 2023 (Kaspersky)



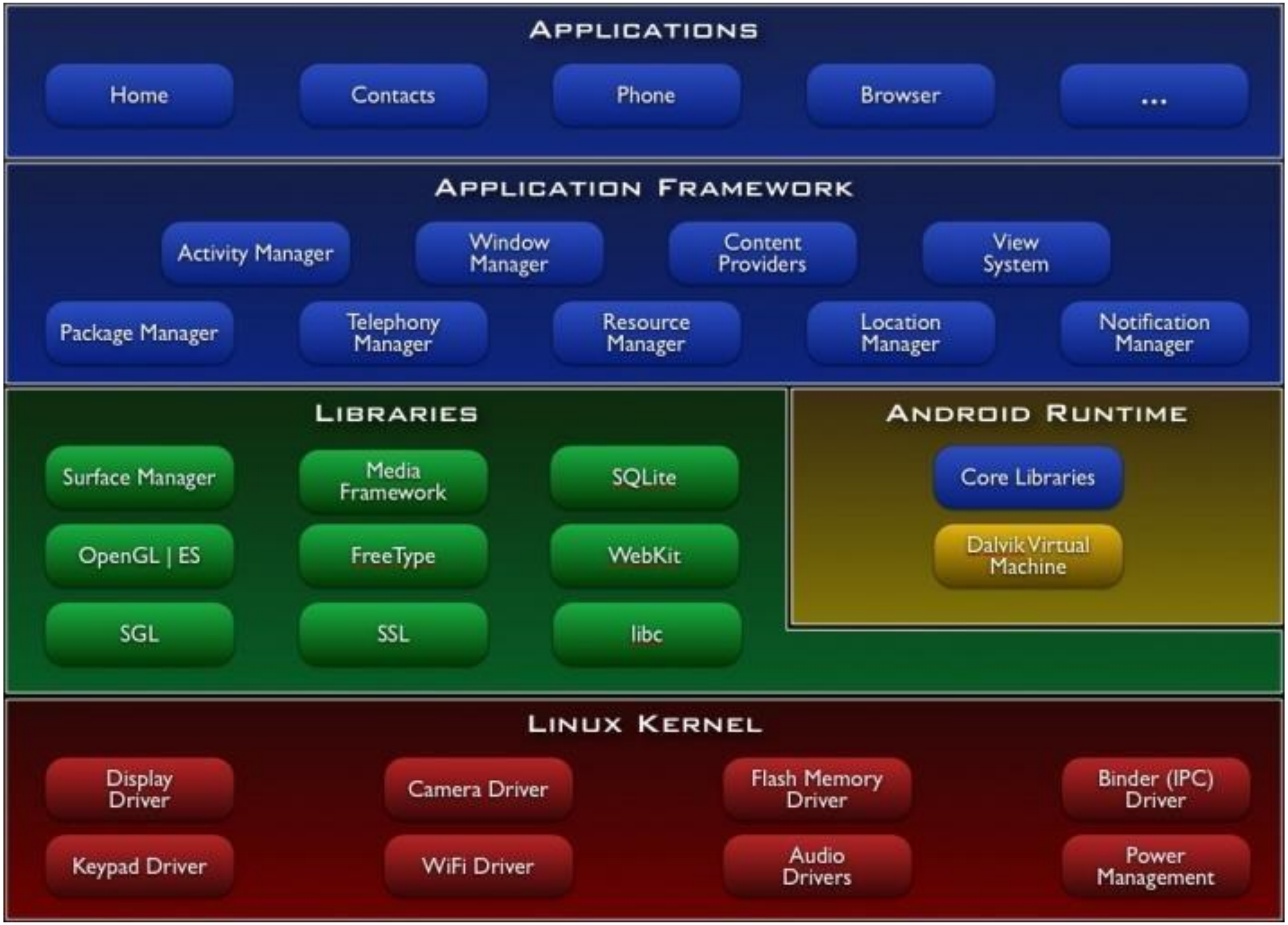
Detected malicious packages

kaspersky

Android Fundamentals

Hacking Your Android

Android Fundamentals



Architecture

- Core is ARM cross-compiled Linux kernel
- Libraries to draw 2D/3D graphics, use GPS, etc.
  - SQLite database engine stores application data on the device without encryption
  - Dalvik Virtual Machine
    - Replaced by ART from Lollipop 5.0 (better performance)
    - Uses **dex** files
  - Java libraries
- Application framework
- Applications

Dalvik Virtual Machine

- Each application runs in its own instance of Dalvik VM
  - Makes applications work on many devices
  - Very limited power, memory, storage
  - Apps are written in Java, transformed to **dex** (Dalvik Executable)
  - Dalvik is open source

Sandbox

- Each application runs in a separate process with a unique User ID
- Apps cannot interact with each other
- Sandbox is implemented in kernel
    - Works for both native and operative system applications

File System Security

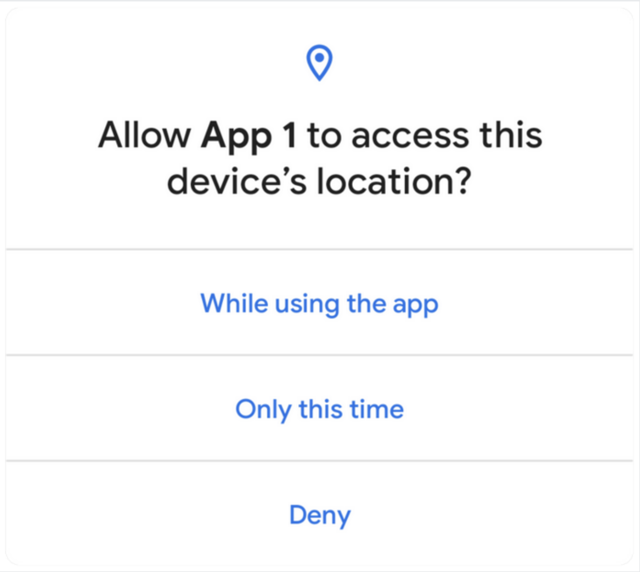
- Android 3.0 and later encrypts file system with AES 128 to protect data on a stolen phone
- System partition is read-only, unless user is root
- Files created by one app can't be modified by a different app
  - Thanks to sandboxing

Memory Security

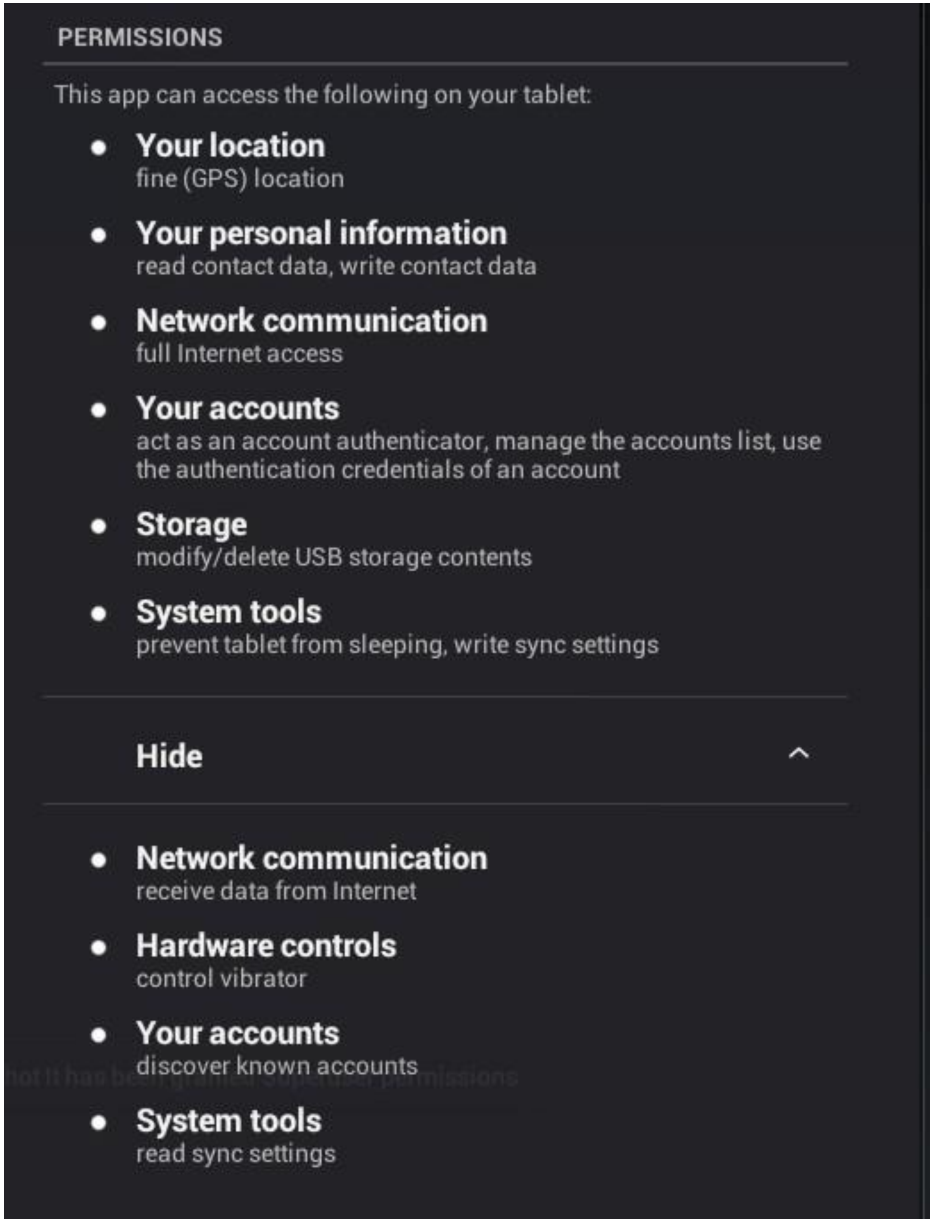
- Address Space Layout Randomization (ASLR)
- NX bit (No eXecute)

Protected APIs

- User must agree to grant an app permissions



Allow **App 1** to access this device's location?



PERMISSIONS

This app can access the following on your tablet:

- **Your location**
  fine (GPS) location
- **Your personal information**
  read contact data, write contact data
- **Network communication**
  full Internet access
- **Your accounts**
  act as an account authenticator, manage the accounts list, use the authentication credentials of an account
- **Storage**
  modify/delete USB storage contents
- **System tools**
  prevent tablet from sleeping, write sync settings

- **Network communication**
  receive data from Internet
- **Hardware controls**
  control vibrator
- **Your accounts**
  discover known accounts
- **System tools**
  read sync settings

Certificates

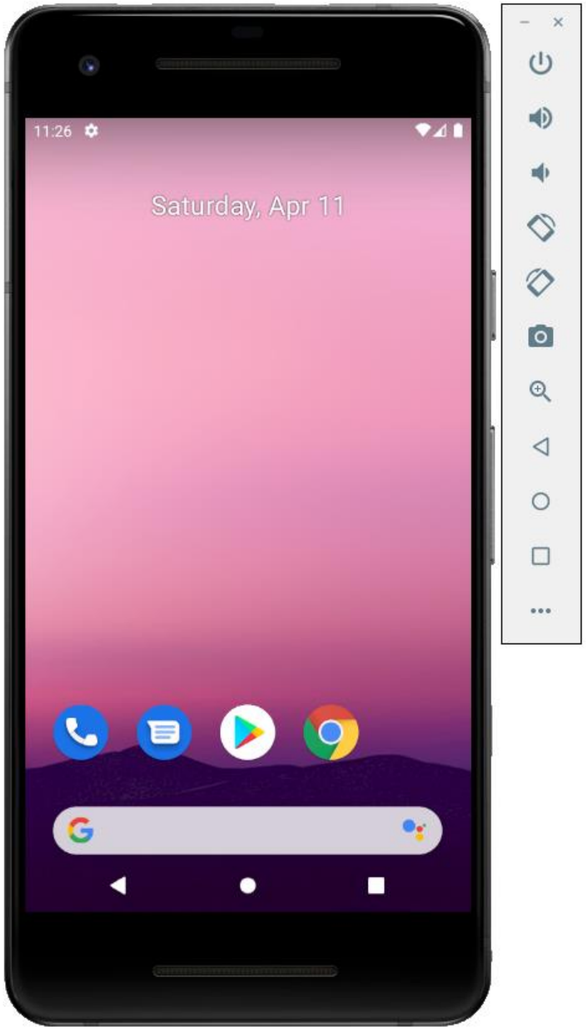
- All apps must be signed with a certificate
- BUT it can be self-signed (no CA)

SDK (Software Development Kit)

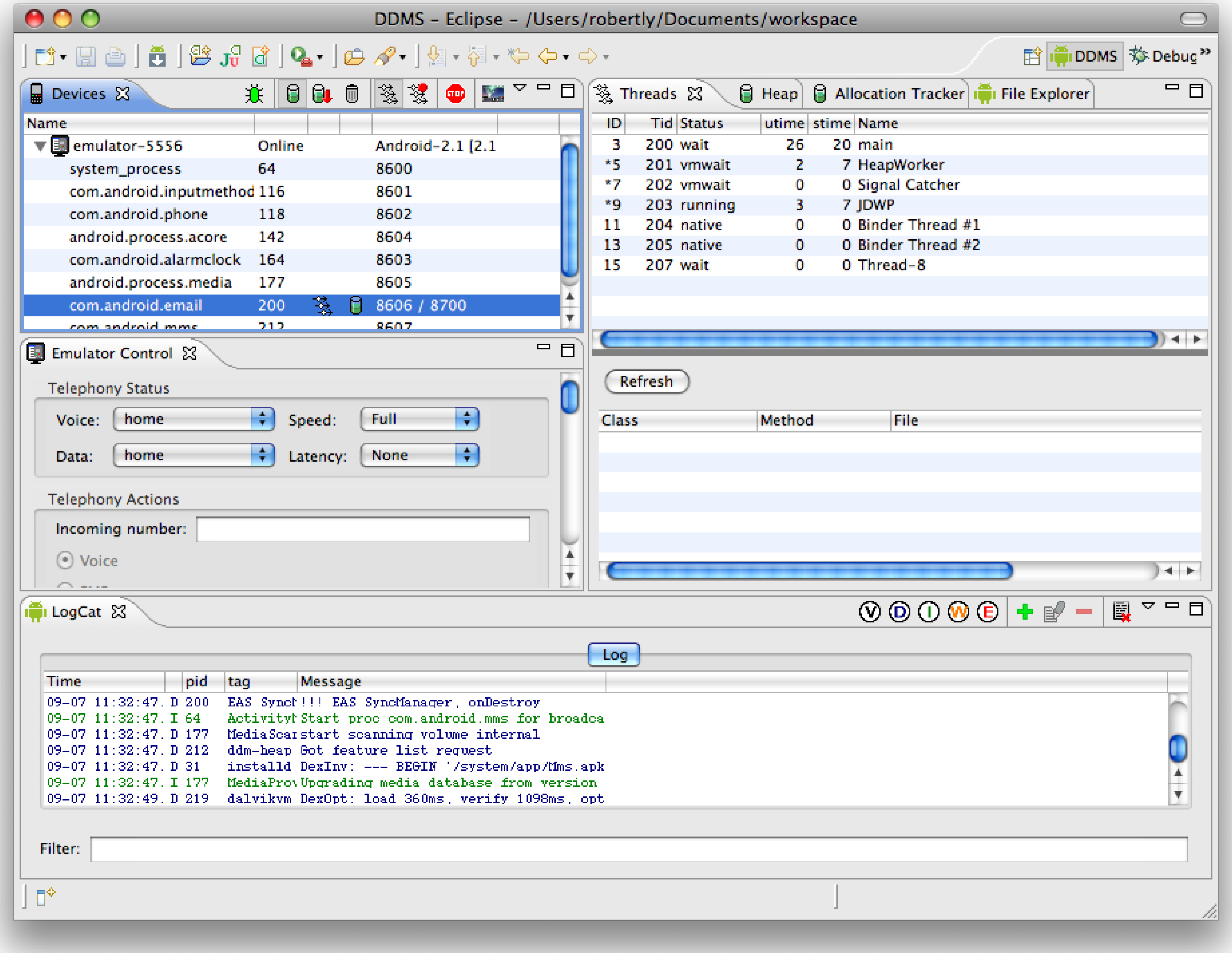
- Android Emulator

  (Image from geeksforgeeks.or)

- Android Debug Bridge
  - Command-line tool to communicate with emulator or physical device (ports 5555 to 5585)
    - **Pull/push:** copies and retrieve files from the device
    - **Install:** install an application in the device
    - **Logcat:** to obtain log data from the screen
    - **Forward:** forwards a specific connection to another port
    - **Shell:** to start a remote shell in the device.



Dalvik Debug Monitor Server



Name		
emulator-5556	Online	Android-2.1 [2.1
system_process	64	8600
com.android.inputmethod	116	8601
com.android.phone	118	8602
android.process.acore	142	8604
com.android.alarmclock	164	8603
android.process.media	177	8605
com.android.email	200	8606 / 8700
com.android.mms	212	8607

ID	Tid	Status	utime	stime	Name
3	200	wait	26	20	main
*5	201	vmwait	2	7	HeapWorker
*7	202	vmwait	0	0	Signal Catcher
*9	203	running	3	7	JDWP
11	204	native	0	0	Binder Thread #1
13	205	native	0	0	Binder Thread #2
15	207	wait	0	0	Thread-8

Class	Method	File

Telephony Status

Voice: home Speed: Full

Data: home Latency: None

Telephony Actions

Incoming number:

○ Voice

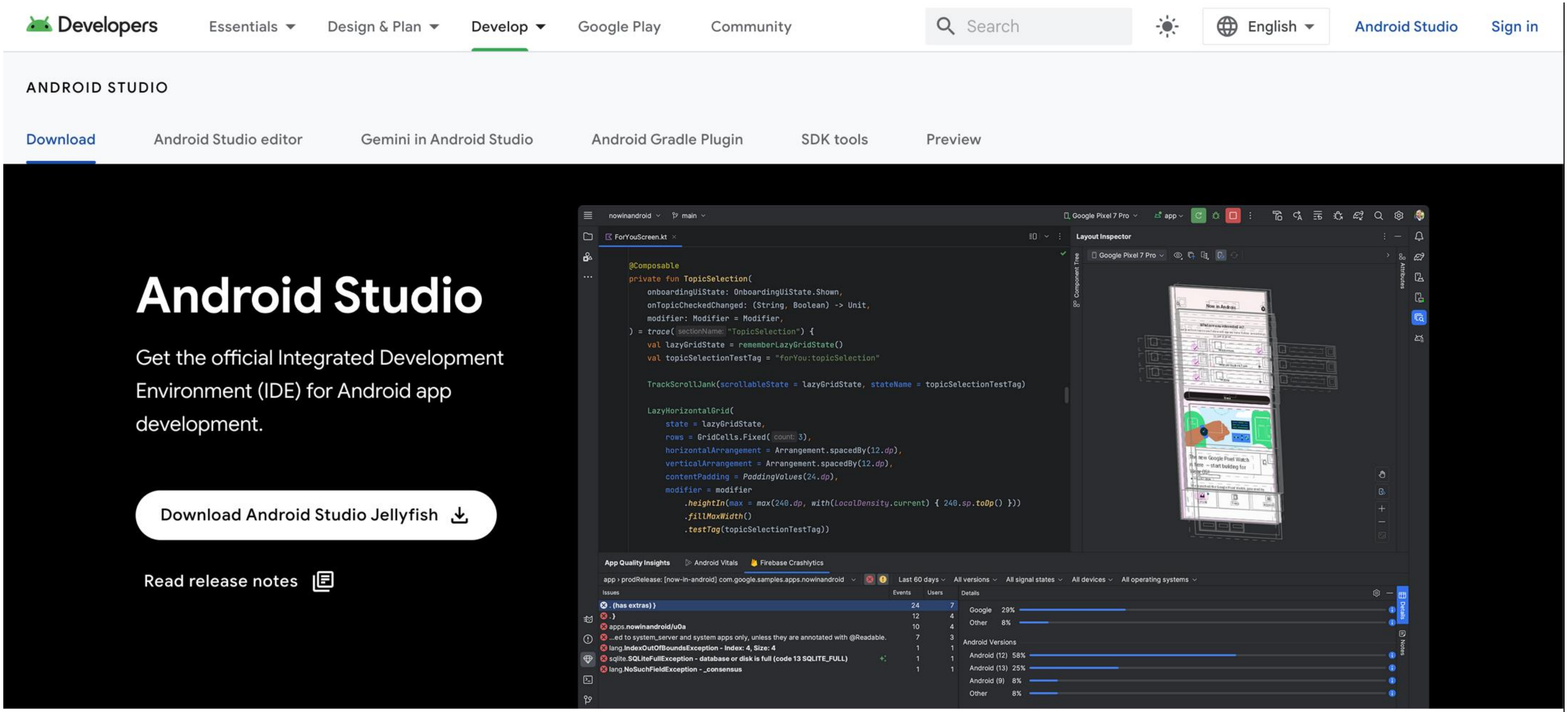
```
Time             pid tag       Message
09-07 11:32:47. D 200  EAS Synct !!! EAS SyncManager, onDestroy
09-07 11:32:47. I 64   Activityt Start proc com.android.mms for broadca
09-07 11:32:47. D 177  MediaScar start scanning volume internal
09-07 11:32:47. D 212  ddm-heap Got feature list request
09-07 11:32:47. D 31   installd DexInv: --- BEGIN '/system/app/Mms.apk
09-07 11:32:47. I 177  MediaProv Upgrading media database from version
09-07 11:32:49. D 219  dalvikvm DexOpt: load 360ms, verify 1098ms, opt
```

Filter:

Deprecated and then removed in Android studio 3.2

Dalvik Debug Monitor Server

- Today: embedded Android Studio features
  - Android profiler
  - Device explorer
  - Debugger window
  - Adb
  - Android emulator



Android Studio

Get the official Integrated Development Environment (IDE) for Android app development.

```
@Composable
private fun TopicSelection(
    onboardingUiState: OnboardingUiState.Shown,
    onTopicCheckedChanged: (String, Boolean) -> Unit,
    modifier: Modifier = Modifier,
) = trace( sectionName: "TopicSelection") {
    val lazyGridState = rememberLazyGridState()
    val topicSelectionTestTag = "forYou:topicSelection"

    TrackScrollJank(scrollableState = lazyGridState, stateName = topicSelectionTestTag)

    LazyHorizontalGrid(
        state = lazyGridState,
        rows = GridCells.Fixed( count: 3),
        horizontalArrangement = Arrangement.spacedBy(12.dp),
        verticalArrangement = Arrangement.spacedBy(12.dp),
        contentPadding = PaddingValues(24.dp),
        modifier = modifier
            .heightIn(max = max(240.dp, with(LocalDensity.current) { 240.sp.toDp() }))
            .fillMaxWidth()
            .testTag(topicSelectionTestTag))
```

Issues	Events	Users
. (has extras) }	24	7
.}	12	4
apps.nowinandroid/u0a	10	4
...ed to system_server and system apps only, unless they are annotated with @Readable.	7	3
lang.IndexOutOfBoundsException - Index: 4, Size: 4	1	1
sqlite.SQLiteFullException - database or disk is full (code 13 SQLITE_FULL)	1	1
lang.NoSuchFieldException - _consensus	1	1

Details

Google	29%
Other	8%

Android Versions

Android (12)	58%
Android (13)	25%
Android (9)	8%
Other	8%

Hacking Android

Android Fundamentals

- Android architecture
  - ARM cross-compiled Linux kernel
  - Native libraries
  - Android runtime (including Dalvik virtual machine)
  - Application framework
  - Applications
- Software Development Kit (SDK)
  - Android Emulator: prototype, develop, and test Android applications without using a physical device
  - Android Debug Bridge (ADB):
    - a command-line tool for communicating with an emulator or a physical device
    - execution of native apps
  - Dalvik Debug Monitor Server (DDMS):
    - obtain log information through logcat
    - send simulated location data, SMS, and phone calls
    - provide memory management information

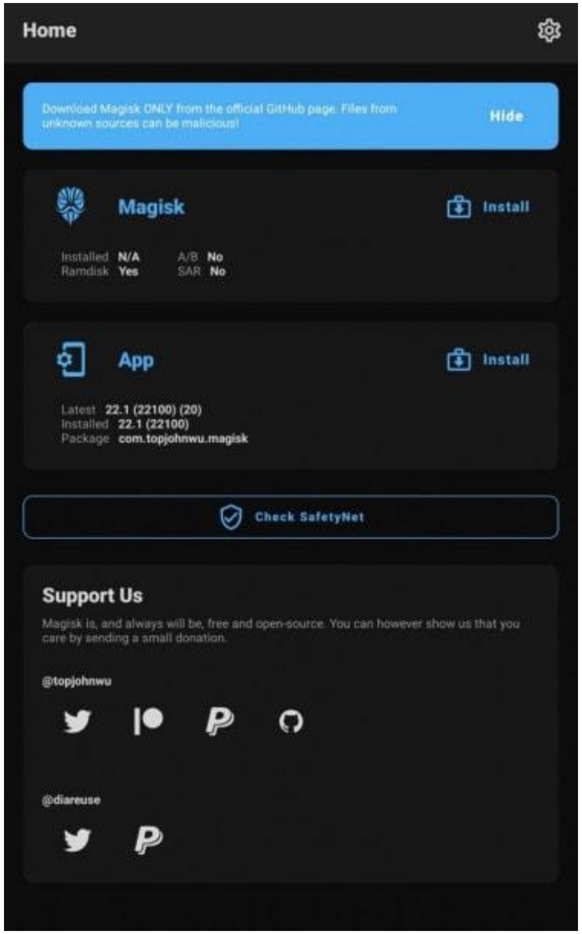
Hacking Your Android

Rooting Android

- Privilege escalation attack
- Exploit a vulnerability to gain root privileges
  - (Called **jailbreaking** on iOS)
- RISKS:
  - Bricking your phone, by corrupting the OS
    - You may need to buy a new phone
  - Compromises security of OS, enabling more malware
    - Rooting tools install SuperUser.apk implementing access control

Magisk

- First, unblock bootleader with adb
- Install magisk
- Modify boot.img file in the device
- https://medium.com/@sarang6489/rooting-android-device-magisk-72e05793a1fb



Download Magisk ONLY from the official GitHub page. Files from unknown sources can be malicious!

Magisk

Installed N/A
Ramdisk Yes
A/B No
SAR No

App

Latest 22.1 (22100) (20)
Installed 22.1 (22100)
Package com.topjohnwu.magisk

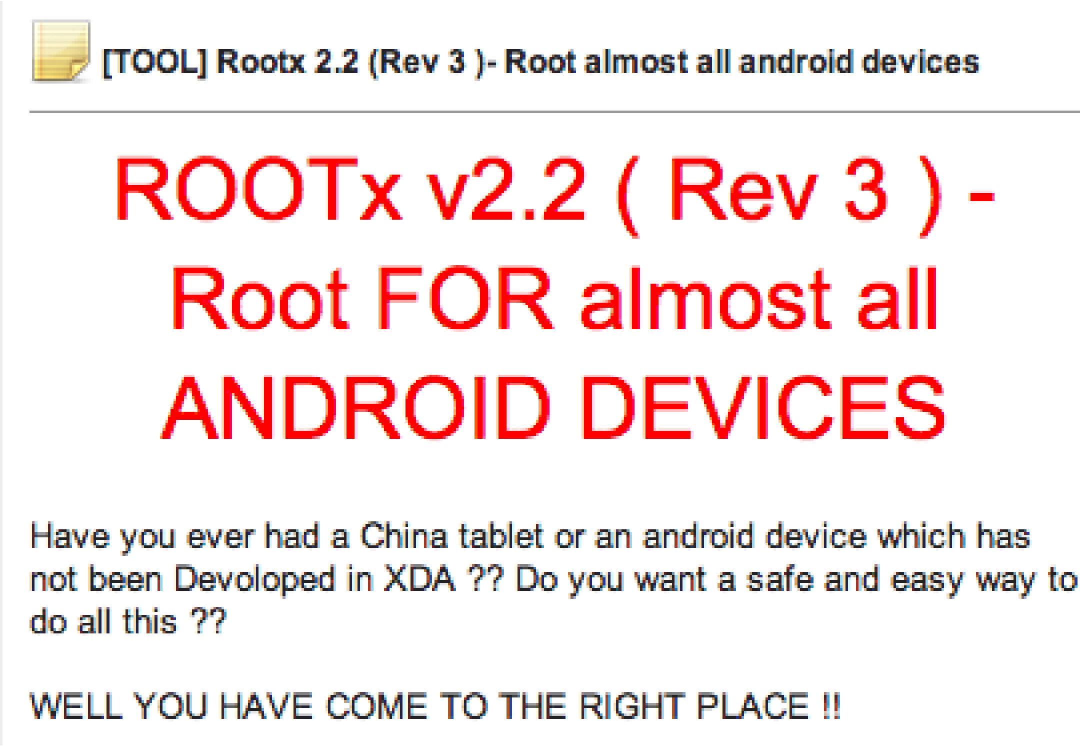
Support Us

Magisk is, and always will be, free and open-source. You can however show us that you care by sending a small donation.

@topjohnwu

@diareuse

ROOTx



[TOOL] Rootx 2.2 (Rev 3)- Root almost all android devices

ROOTx v2.2 (Rev 3) - Root FOR almost all ANDROID DEVICES

Have you ever had a China tablet or an android device which has not been Devoloped in XDA ?? Do you want a safe and easy way to do all this ??

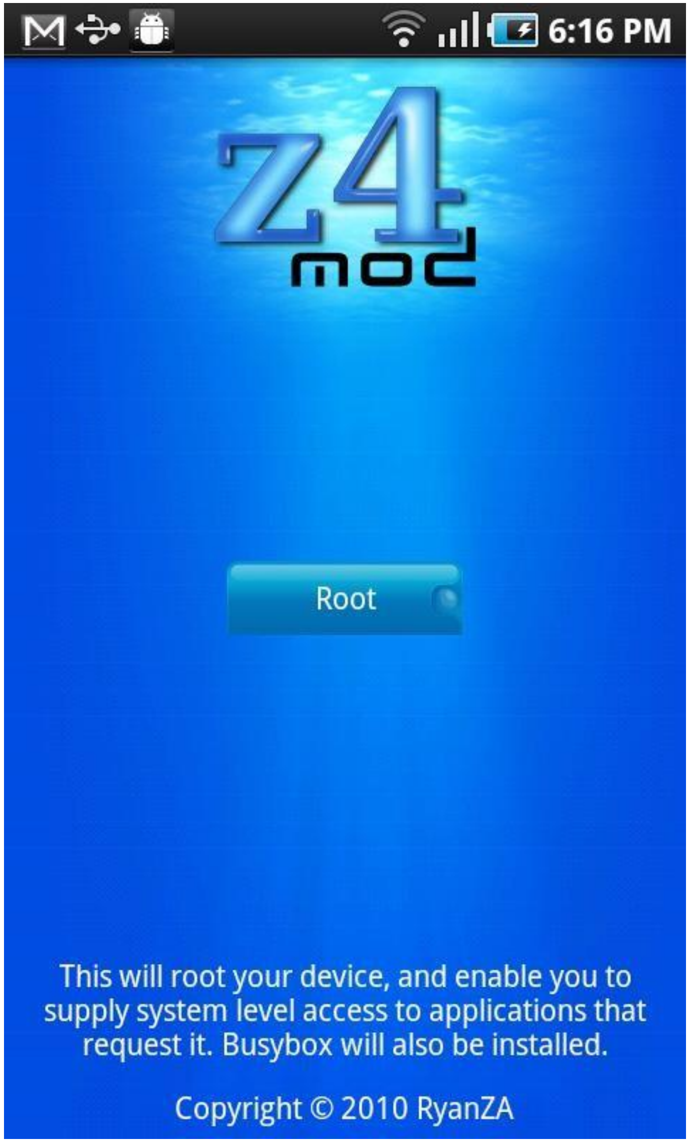
WELL YOU HAVE COME TO THE RIGHT PLACE !!

Android Rooting Tools

- SuperOneClick
  - Native Windows application, runs on Linux and Mac with Mono
    - https://www.mono-project.com/
  - Run SuperOneClick on a computer
  - Connect phone with USB cable
  - Turn on "USB Debugging"
  - Most universal

Android Rooting Tools

- Z4Root
  - Android app



This will root your device, and enable you to supply system level access to applications that request it. Busybox will also be installed.

Copyright © 2010 RyanZA

Android Rooting Tools

- GingerBreak
  - Doesn't work on all devices

Rooting a Kindle Fire

- Kindle Fire OS v1 is a customized version of Android 2.3
- Cannot access the Android Market
- BurritoRoot
- Newer versions: https://www.lifewire.com/how-to-root-kindle-fire-4684526

Hacking Your Android

Hacking Your Android

- Rooting “your” Android to get administrative privileges
  - Full control of the device
  - The device may be “bricked”
- Android Rooting Tools: SuperOne Click, Z4Root, GingerBreak
- Steps for rooting a Kindle Fire
  - Enable installation of applications from unknown sources
  - Install the Android SDK
  - Add commands in *adb_usb.in* and *android_winusb.inf*
  - Connect Kindle Fire with PC through ADB
  - Download rooting files and execute them

Cool Apps for Rooted Android

- Superuser
  - Controls applications that use root privileges
  - Pops up asking for permission each time an app uses the su binary
- ROM Manager
  - Manage custom ROMS, so you can have the latest Android version on your device

Cool Apps for Rooted Android

- Market Enabler
  - Lets you use apps that are restricted to certain countries, regions, or carriers
- ConnectBot
  - SSH client
- ES File Manager
- SetCPU
  - Overclock or underclock

Hacking Your Android

Apps for Rooted Android Devices

- Superuser: control which applications can execute with root privileges
- ROM Manager: install a custom ROM
- Market Enabler: spoof your location and carrier network to the Android market
- ConnectBot: execute shell commands remotely
- ES File Manager: copy, paste, cut, create, delete, and rename system files
- SetCPU: set the CPU clock
- Juice Defender: save power and extend battery life by managing hardware components

Native Apps on Android

- Linux pros: Open source tools already available for Linux
- A **cross compiler** is a compiler capable of creating executable code for a platform other than the one on which the compiler is running. For example, a compiler that runs on a Windows PC but generates code that runs on Android smartphone is a cross compiler.
  - Compile open source Linux tools for Android (for attacks?)
  - Develop apps (exploits?) on a PC, and compile them for ARM
- Android Native Development Kit in SDK
  - Lets you develop apps for the Dalvik Virtual Machine

Hacking Your Android

Precompiled binary tools on Android

- BusyBox: a set of UNIX tools that allows you to execute useful commands, like tar, dd, wget
- Tcpdump: capture in PCAP file and display packets that are transmitted over a network
- Nmap: discover hardware and software on a network to identify specific details of the host operating system, open ports, DNS names, and MAC addresses,
- Ncat: read and write data across networks from the command line for making various remote network connections

Trojan Apps

- Easy to insert a malicious code inside legitimate APK files (Android Applications)
- Open APK with 7-zip
  - Manifest
    - XML file defining SW components and permissions
  - Classes.dex
    - Dalvik executable with compiled code

App Entry Points

- Android apps may have more entry points
- Broadcast receiver
  - Enables apps to receive "intents" from system
  - Like interrupts
  - Example: Run when an SMS is received
- Services
  - Run in background, no GUI shown to user

App Re-packaging

Android trojan app process:

- take a legitimate application, disassemble the dex code, decode the manifest.
- include the malicious code, assemble the dex, encode the manifest,
- sign the final apk file.
- One tool available is apktool
  - https://apktool.org/

apktool

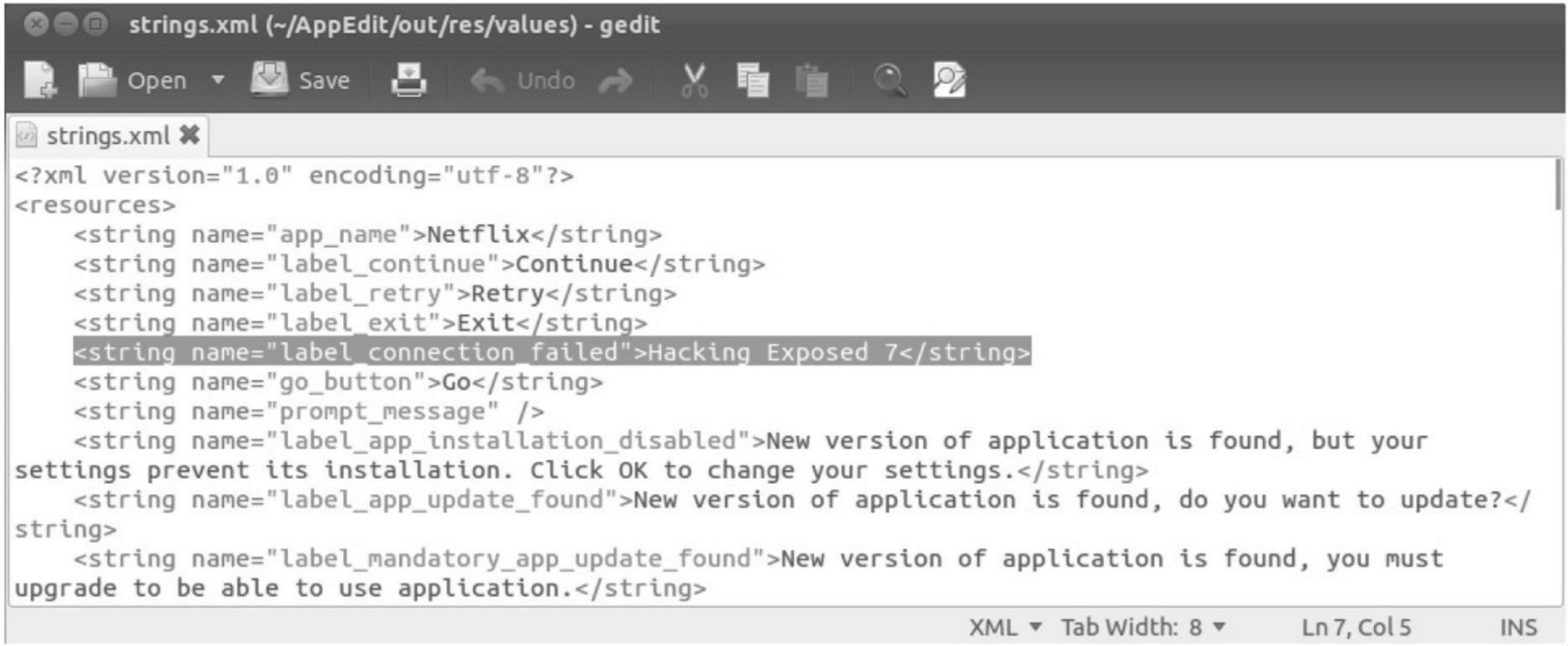
android-apktool

A tool for reverse engineering Android apk files

- Disassembles dex code into **smali**
  - Raw Dalvik VM bytecode
- Can be used to embed malicious code into apps

Example Netflix

- Netflix.apk application modified.
- The label “Hacking Exposed 7” appears when a «Conection failure» error occurs.



```
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="app_name">Netflix</string>
    <string name="label_continue">Continue</string>
    <string name="label_retry">Retry</string>
    <string name="label_exit">Exit</string>
    <string name="label_connection_failed">Hacking Exposed 7</string>
    <string name="go_button">Go</string>
    <string name="prompt_message" />
    <string name="label_app_installation_disabled">New version of application is found, but your
settings prevent its installation. Click OK to change your settings.</string>
    <string name="label_app_update_found">New version of application is found, do you want to update?</
string>
    <string name="label_mandatory_app_update_found">New version of application is found, you must
upgrade to be able to use application.</string>
```

Hacking Your Android

Trojan Apps

- A malicious program that disguises legitimate apps by using the same icon or name
- Reengineer Android applications
  - Manifest.xml: an encoded XML file that defines essential information about the application to the Android
  - Classes.dex: the Dalvik executable where the compiled code resides
- Tools for Modify an app
  - apktool: unzip and repack the Android application (apk) file
  - SignApk: verify the repacked file

Hacking Other User’s Androids

Vulnerable targets due to fragmentation of the Android platform

Remote Shell via WebKit

- WebKit is an open-source Web browser engine
- Vulnerability: handled floating point data types incorrectly (patched in Android 2.2)
- Drive-by download from a malicious Web server hosting a malicious HTML file.
- Access to HTML file returns a remote shell (but not root)
- Countermeasures: updates & antivirus

Root Exploits

- How to gain root on the exploited device?
- **exploid**
- **RageAgainstTheCage**

- Countermeasures: Updates & Antivirus

Data Stealing Vulnerability

- A malicious website can steal data from the SD card and from the device itself
  - As long as root privileges not required
- User must click a malicious link
  - Exploit is a PHP file with embedded JavaScript
  - User sees a notification, which may warn them
  - Attacker must know name & path to file (WebKit vulnerability can be used)

Data Stealing Vulnerability Countermeasures

- Use latest version of Android
  - CyanogenMod custom ROM enables you to use a new version even if your carrier blocks the update
- Install antivirus
- Temporarily Disable JavaScript
- Use a third-party browser like Firefox or Opera
- Unmount sdcard

Remote Shell with Zero Permissions

- Using carefully chosen functions, it's possible to open a remote shell with no permissions from the user
- Works in all versions of Android, even 4.0, Ice Cream Sandwich
- Thomas Cannon https://vimeo.com/33576202
  - REBOOT permission: can be bypassed with a DoS attack by generating multiple Toasts
  - INTERNET: can be bypassed by launching an invisible browser. To receive data, custom URI receiver in the manifest (BROWSABLE category)
  - Get sensitive data through READ_LOG permission to gather data through other permissions

Capability Leaks

- Stock software exposes permissions to other applications
- Enables untrusted apps to gain privileges the user didn't allow
- **Explicit leaks**: Access public interfaces or services that have the permission that the untrusted application does not have.
- **Implicit leakes**: Untrusted application acquired the same permissions of the privileged application because they share the same signing key

URL sourced malware

- Apps can be also installed from the web browser by downloading .apk files
- Zeus and Spyeye (Trojan Banking apps)
  - Injects a malicious frame in the computer web browser, steals the credentials and displays a web page encouraging the user to click a URL pointing to a Trojan apk file
  - The trojan intercepts all the SMS messages received in the device and shunts them to a remote server
  - Bypasses SMS two-factor authentication

URL sourced malware

countermeasures

- Do not allow apks from unknown sources
- Some carriers disable this feature, by default, and it can’t be enabled without root privileges.

Carrier IQ

- Pre-installed on devices
- Monitors activity and sends it back to the carrier
- Not entirely malicious, intended to improve performance by measuring diagnostic data
- Huge privacy controversy
    - For example, IMIEI and geographical positiojn might be sent to the Carrier
- Apple was "phasing it out" in 2011
- It's a form of rootkit

Carrier IQ

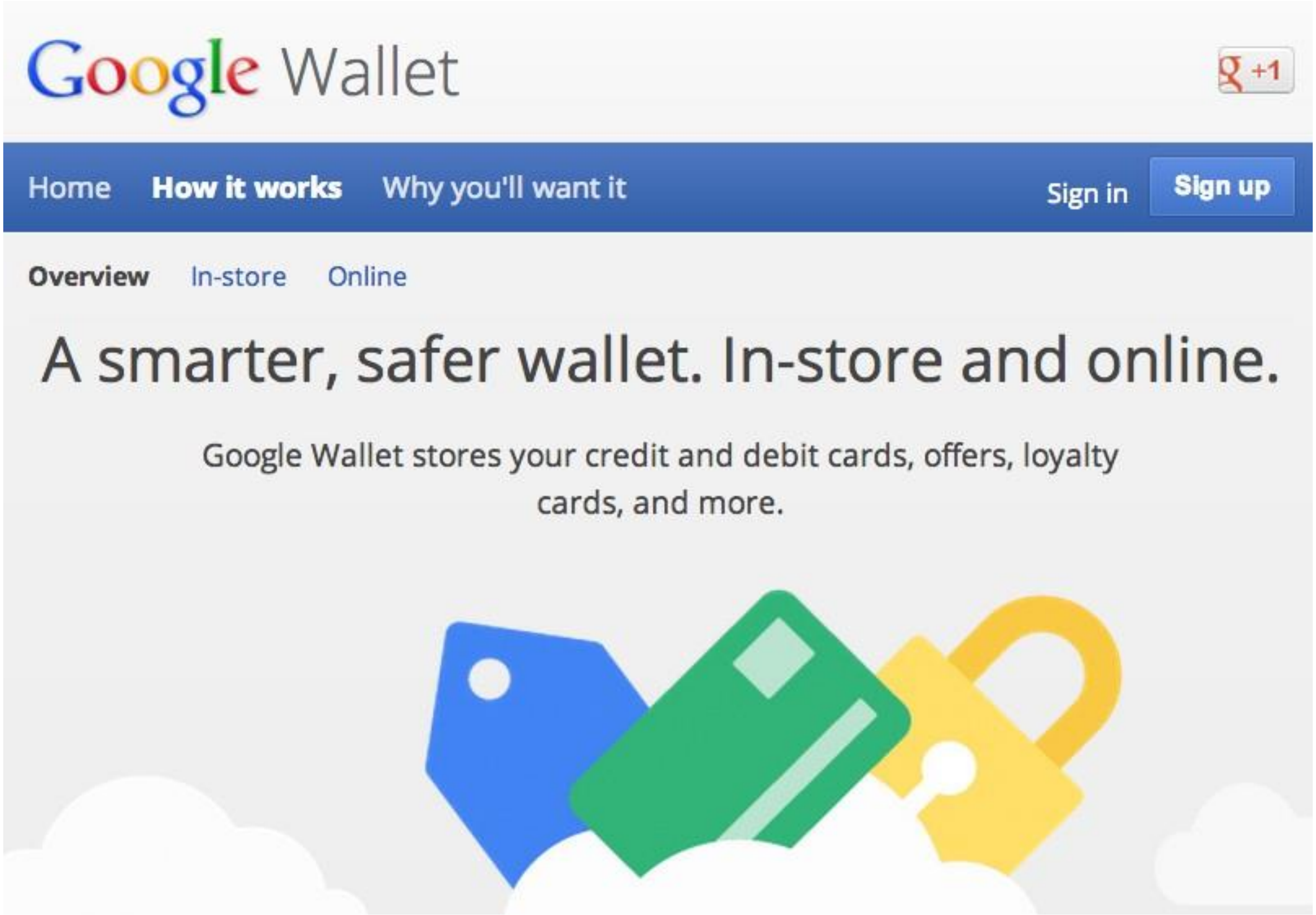
- Countermeasure
  - If installed, use removal kit on rooted phone (might be dangerous)

HTC Logger

- Prealoded manufacturer applications that use logcat to process sensitive information like the content of an SMS or keystrokes
- Vulnearbility in old versions of HTC devices
- **htcloggers.apk**, collected sensitive data, such as geographical location, user data such as e-mail addresses, phone numbers, SMS data and system logs like logcat
  - Opens a local port
  - Any application with INTERNET had access

HTC Logger

- Contermeasures
  - Remove HTC logger with rooted phone
  - Patch



Google Wallet

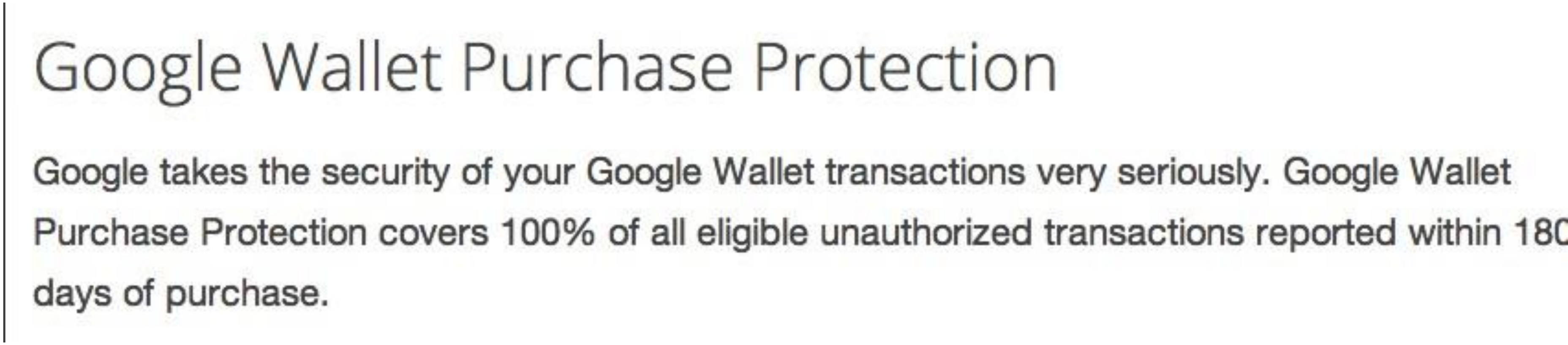
A smarter, safer wallet. In-store and online.

Google Wallet stores your credit and debit cards, offers, loyalty cards, and more.

Google Wallet PIN

- Currently works on almost every phone
- Stores encrypted data in a Secure Element (SE)
- Requires user-defined 4-digit PIN
  - Five incorrect PIN entries locks the application
- But PIN is not in the SE
  - Hashed PIN can be broken by brute-force
- Countermeasure: Don't root your Wallet phone
- **Also HTC Logger**

Protect against fraud



Google Wallet Purchase Protection

Google takes the security of your Google Wallet transactions very seriously. Google Wallet Purchase Protection covers 100% of all eligible unauthorized transactions reported within 180 days of purchase.

Android as a Portable Hacking Platform

Android Hacking Tools

- Network sniffer (Shark for Root)
  - Cross-compiled tcpdump
  - Captures packets in a .pcap file
- Network Spoofer (ARP spoofing)
- Connect Cat (like netcat)
- Nmap for Android

Defending Your Android

- Maintain physical security
- Lock your device (PIN or password)
- Avoid installing apps from unknown sources
- Install antivirus software
- Enable full internal storage encryption
  - Available in Android 3.0 and later
- Update to latest Android version
  - May require custom ROM

iOS

iOS History

- 1980s
  - Steve Jobs, expelled from Apple, founded NeXT
  - NeXTSTEP was the OS of workstation
  - Derived from Carnegie Mellon Universities' CMU Mach kernel plus BSD Unix
  - Used Objective-C for applications

iOS History

- 1996
  - Apple purchased NeXT
  - NeXTSTEP renamed OPENSTEP
  - Modified to adopt Mac OS 9 styling
- 2001
  - Mac OS X released

iOS History

- 2007
  - iPhone introduced, with iPhone OS
  - Later renamed to iOS, confusingly similar to Cisco's IOS
  - iOS is derived from Mac OS X:

    Mach/BSD-based

    Uses Objective-C

iOS Devices

- iPhone
- iPod Touch
- Apple TV
- iPad

Hacking focus changes:

- All use 32-bit ARMv6 or ARMv7 processor
- Objective-C

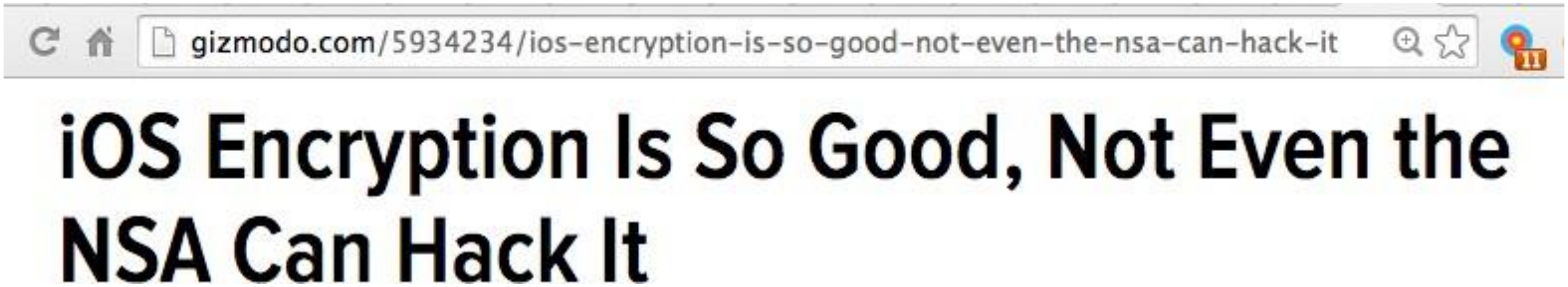
How Secure is iOS?

- Originally iPhone allowed no third-party apps at all
- Since 2008, the App Store appeared
- Early iOS versions were very insecure
  - All apps ran as root
  - No sandbox
  - No code signing
  - No ASLR
  - No Position Independent Executable (PIE) support

How Secure is iOS?

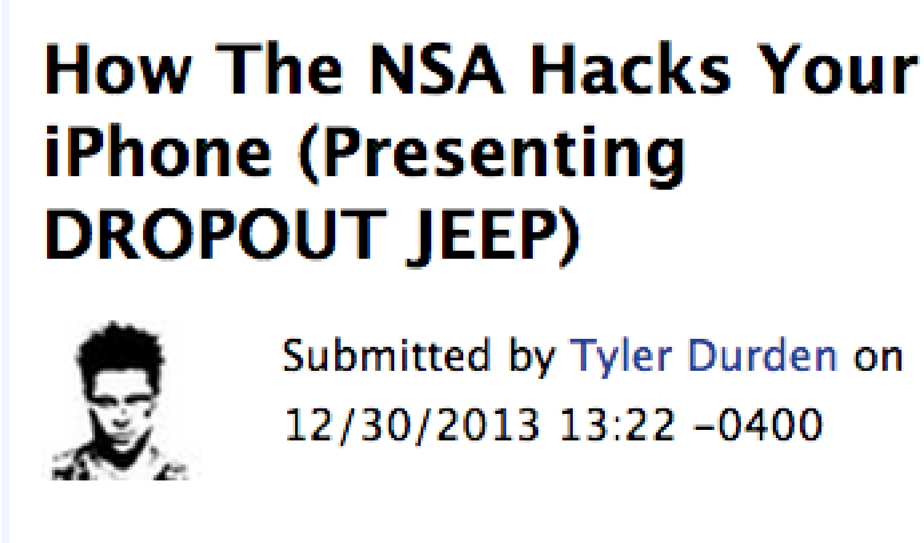
- Security Measures Added in Later Versions
  - Third-party apps run as less privileged account "mobile", not root
  - Sandboxing limits apps to a limited set of system resources
  - Apps have to be signed by Apple to execute
  - Code signature verification is at load time and runtime
  - ASLR for system components and libraries
  - PIE causes apps to load at different base address upon every execution

iPhone Encryption



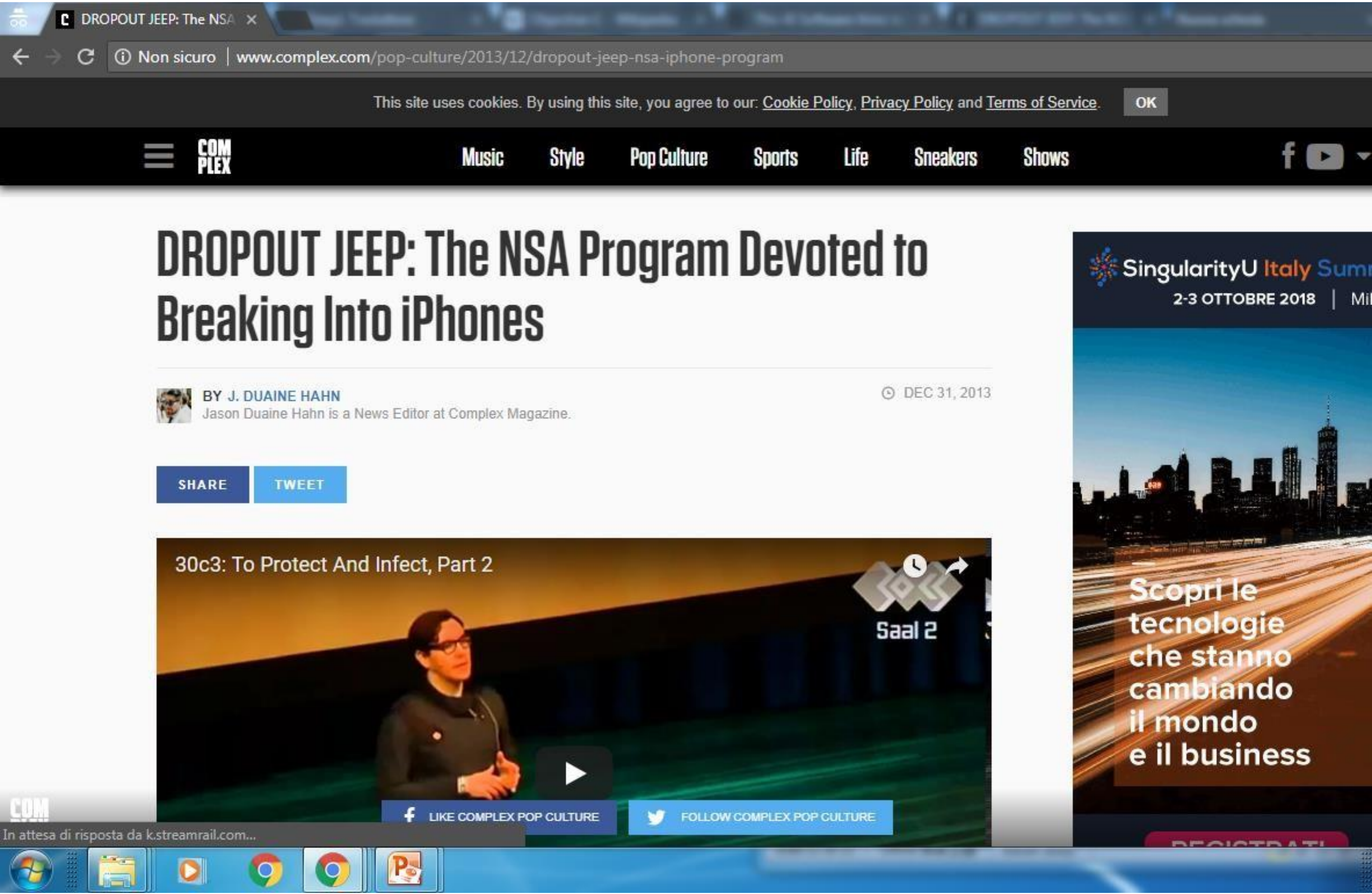
gizmodo.com/5934234/ios-encryption-is-so-good-not-even-the-nsa-can-hack-it

iOS Encryption Is So Good, Not Even the NSA Can Hack It



How The NSA Hacks Your iPhone (Presenting DROPOUT JEEP)

Submitted by Tyler Durden on 12/30/2013 13:22 -0400



DROPOUT JEEP: The NSA ×

Non sicuro | www.complex.com/pop-culture/2013/12/dropout-jeep-nsa-iphone-program

This site uses cookies. By using this site, you agree to our: Cookie Policy, Privacy Policy and Terms of Service. OK

DROPOUT JEEP: The NSA Program Devoted to Breaking Into iPhones

BY J. DUAINE HAHN
Jason Duaine Hahn is a News Editor at Complex Magazine.

DEC 31, 2013

30c3: To Protect And Infect, Part 2

In attesa di risposta da k.streamrail.com...

iPhone 3GS

- The iPhone 3GS was the giant leap forward in encryption
- AES encryption on by default
- Encryption is very fast
- Key is stored in flash memory, but locked with user's PIN
  - Data wipe after 10 guesses is an optional feature

Jailbreaking

What is Jailbreaking?

- Taking full control of an iOS device
- Allows
  - Customization of the device
  - Extensions to apps
  - Remote access via SSH or VNC
  - Arbitrary software
  - Compiling software on the device

Risks of Jailbreaking

- Worries about trojans in jailbreak apps
  - Never yet observed for well-known jailbreak apps
- Jailbroken phones lose some functionality
  - Vendors can detect jailbreaks and block function
  - iBooks did this
- Code signature verification is disabled by jailbreaking
- Expose yourself to a variety of attack vectors

Boot-based Jailbreak Process

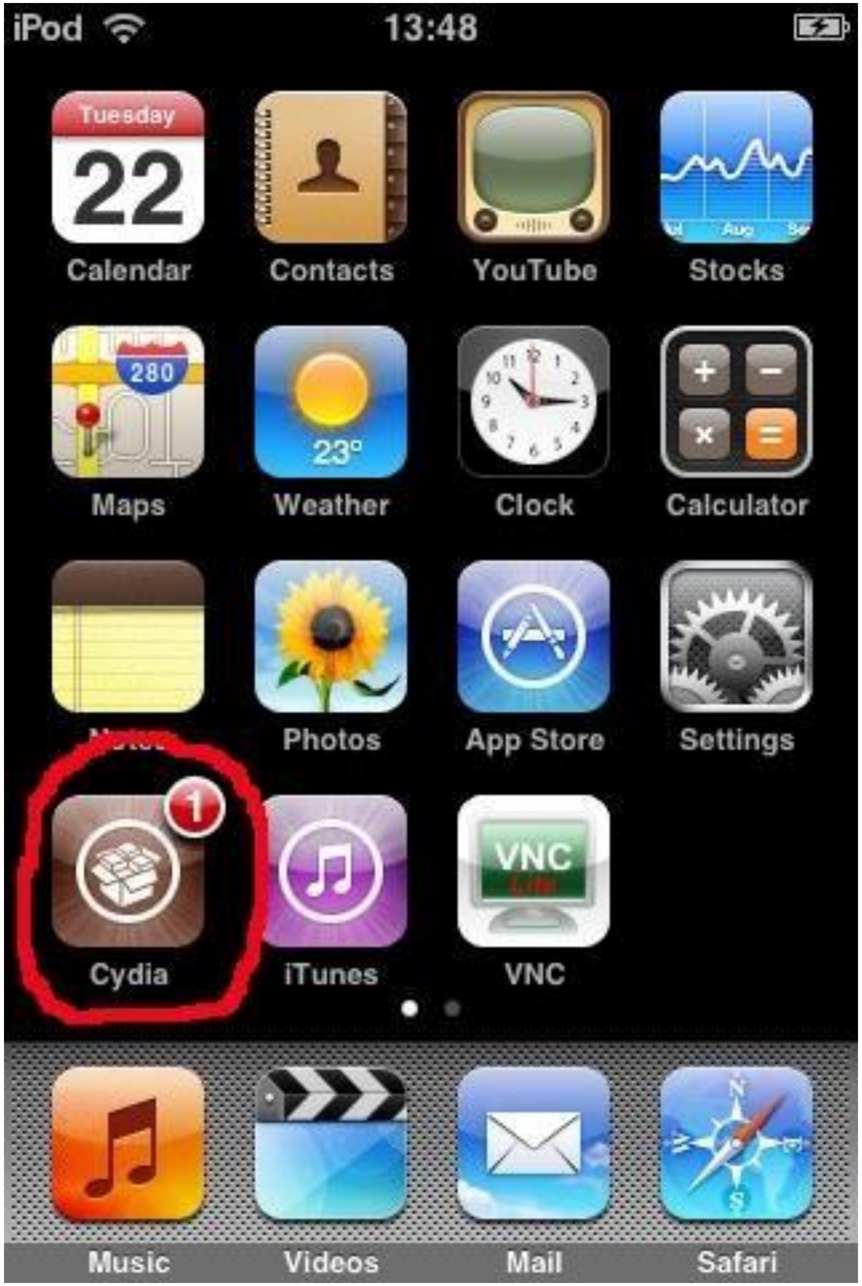
- Obtain firmware image (IPSW) for iOS version and device model
  - From Apple servers
- Obtain jailbreak software
  - redsnow, greenpoison, limera1n
- Connect computer to iphone with USB cable
- Launch jailbreak app

Boot-based Jailbreak Process

- Select IPSW and wait for customizing
- Switch iPhone into Device Firmware Update (DFU) mode
  - Power iPhone off
  - Hold Power+Home buttons for 10 sec.
  - Release Power but hold Home down for 5-10 more seconds
- Jailbreak software completes the process

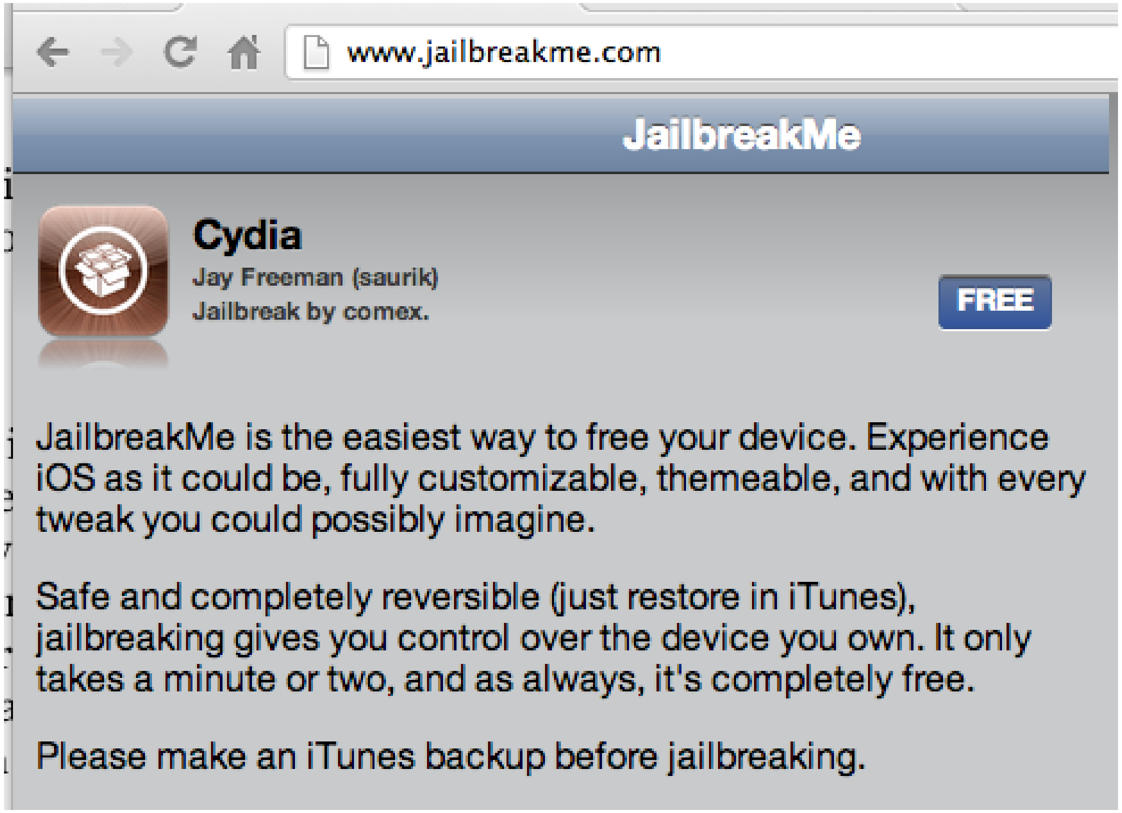
Cydia

- The App Store for jailbroken devices
  - Image from bindapple.com



Remote Jailbreak

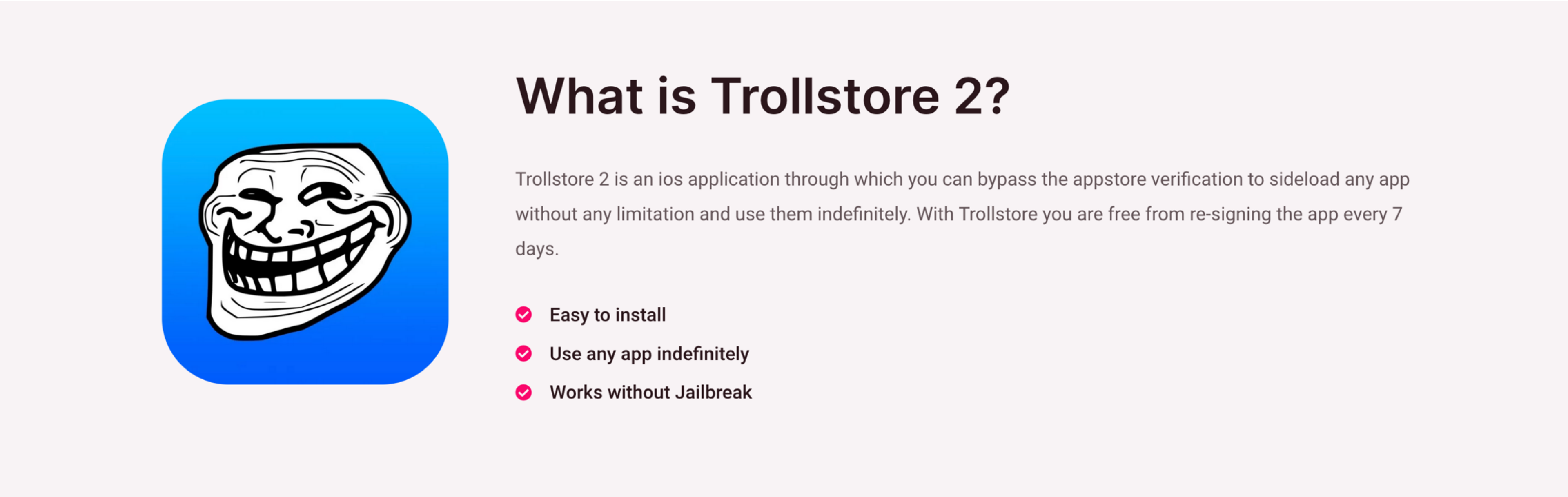
- Jailbreakme.com
  - Just load a PDF file
  - It exploits MobileSafari and jailbreaks the OS
  - Much easier than boot-based jailbreak



JailbreakMe is the easiest way to free your device. Experience iOS as it could be, fully customizable, themeable, and with every tweak you could possibly imagine.

Safe and completely reversible (just restore in iTunes), jailbreaking gives you control over the device you own. It only takes a minute or two, and as always, it's completely free.

Please make an iTunes backup before jailbreaking.



What is Trollstore 2?

Trollstore 2 is an ios application through which you can bypass the appstore verification to sideload any app without any limitation and use them indefinitely. With Trollstore you are free from re-signing the app every 7 days.

- ✓ **Easy to install**
- ✓ **Use any app indefinitely**
- ✓ **Works without Jailbreak**

Hacking Other iPhones

Attack Options

- Local network-based attacks
  - Wireless MITM requires physical proximity
- Attacker with physical access to device
  - Boot-based jailbreak
- Client-side attacks
  - App vulnerabilities, mainly MobileSafari
  - Far more practical
  - But exploiting an app only grants access to data in the app's sandbox

Attack Options

- Breaking out of the sandbox
  - Requires a kernel-level vulnerability

- Exploits used in Jailbreakme can be re-purposed for attack tools

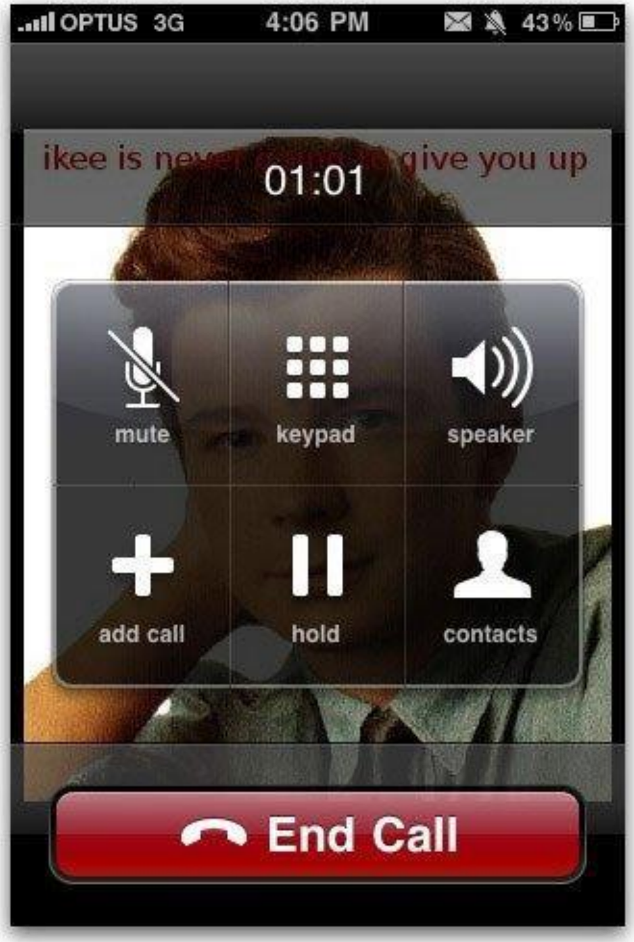
Jailbreakme3.0 Vulnerabilities

- Uses a PDF bug and a kernel bug
- Techniques similar can be used for malicious perposes?

- Countermeasure: Update iOS to latest version
- If you jailbreak, you can't update iOS
- In order to jailbreak, you must use a vulnerable iOS version

iKEE Attacks!

- People jailbroke iPhones, installed OpenSSH, and left the default password 'alpine' unchanged
- 2009: First iPhone worm rickrolled victims
- Later versions made an iPhone botnet



iPhone Remote Attacks

- If you don't jailbreak your iPhone, it's very safe
- Only one port is open
  - TCP 62087
  - No known attacks
  - Tiny attack surface
  - No SSH, SMB, HTTP…
- Almost impossible to gain unauthorized access from the network

Remote Vulnerabilities

- ICMP request causes device reset
  - CVE-2009-1683
- SMS message arbitrary code execution exploit
  - By Charlie Miller
    - Image from techpatio.com
  - CVE-2009-2204

iKee Worm Countermeasures

- Don't jailbreak!
- Change the password
- Enable SSH only when needed
  - SBSettings makes this easy
- Upgrade iOS to the latest jailbreakable version
- Install patches made available by the community

FOCUS 11 Wireless MITM Attack

- Malicious wireless access point simulated with a Mac laptop and two network cards in 2011 Conference in Las Vegas
- Certificate chain validation vulnerability exploited to MITM SSL connections
- PDF used JailBreakMe3.0 attack to silently root the device
- SSH and VNC installed

Countermeasures

- Possible to take full control of iPhone

- Update iOS bundle
- Configure your iPhone to "Ask to Join Networks"
- Don't store sensitive data on your phone

Malicious Apps

- Handy Light
  - 2010
  - Supposedly a flashlight
  - Contained a hidden tethering feature
  - Apple removed it once they found out
- InstaStock
  - Posed as stock-market tracker, but ran unsigned, unauthorized code
  - From Charlie Miller

Malicious Apps Countermeasures

- Apps first submitted to Apple store for review.
- Code may be hidden from the Apple review
- Apple doesn't allow antivirus in the Apple store

- Update firmware
- Apps should be installed only when absolutely necessary and only from trustworthy vendors

Vulnerable Apps

- Citi Mobile app vuln
  - Stored banking data on the iPhone
  - Information disclosure risk if phone stolen
  - CVE-201-02913
- PayPal App
  - X.509 certificate validation missing
  - Allowed MITM attacks
  - CVE-2011-4211

Vulnerable Apps

- Skype XSS
  - Embed JavaScript in FullName
  - Countermeasues

  Keep your device updated with the latest version of iOS, and keep apps updated to their latest versions

Physical Access

- Boot-based jailbreak
- Install SSH server
- Access to data, including passwords in keychain
  - Takes 6 min. to do

Countermeasures

- Encrypt data using Apple features and third-party tools from McAfee, Good, etc.
- Use a passcode of 6 digits or more
- Install remote-tracking software to recover a stolen or lost device, or remotely wipe it

Mobile Hacking Summary

- Adapt the behavior and configuration of the device to your purpose/data after evaluation
- Enable device lock, clean touch-screen
- Keep physical control of the device
- Enable wipe functionality as appropriate using local or remote features
- Install MDM (Mobile Device Management)
- Keep software up to date
- “ask to join” wifi network
- Leave the device home when traveling abroad

Homework Ch11

(format: problem, solution with explanation, screen dumps)

1. (60 points) Android Debug Tool
   1) Install Android SDK.
   2) Connect an Android device or emulator to the host which runs DDMS in the SDK.
   3) Dump and explain contents output by logcat in DDMS.
2. (40 points) Select an Android device or emulator (e.g. the one in Android SDK, Bluestacks, and so on), root it. It is recommended to root on an Android emulator to avoid turning your phones "bricked".
3. (20 points) Use document management app (e.g. Root Explorer) to add/remove apk files to/from the folder “/system/app/” in a rooted Android device or emulator, and observe what happens.
4. (20 points) Install the app, AdBlock, in an rooted Android device or emulator and explain how it blocks Ads.
5. (20 points) Install a root-dependent app (except AdBlock) to a rooted Android device or emulator and explain why it needs a root system.
6. (20 points) Select one version of iOS, survey how to jailbreak it, and list the steps.