

Análisis estático y comparativa de apps iOS provenientes de diferentes mercados de apps

Adrián Campazas Vega

11 de Septiembre de 2019

Índice

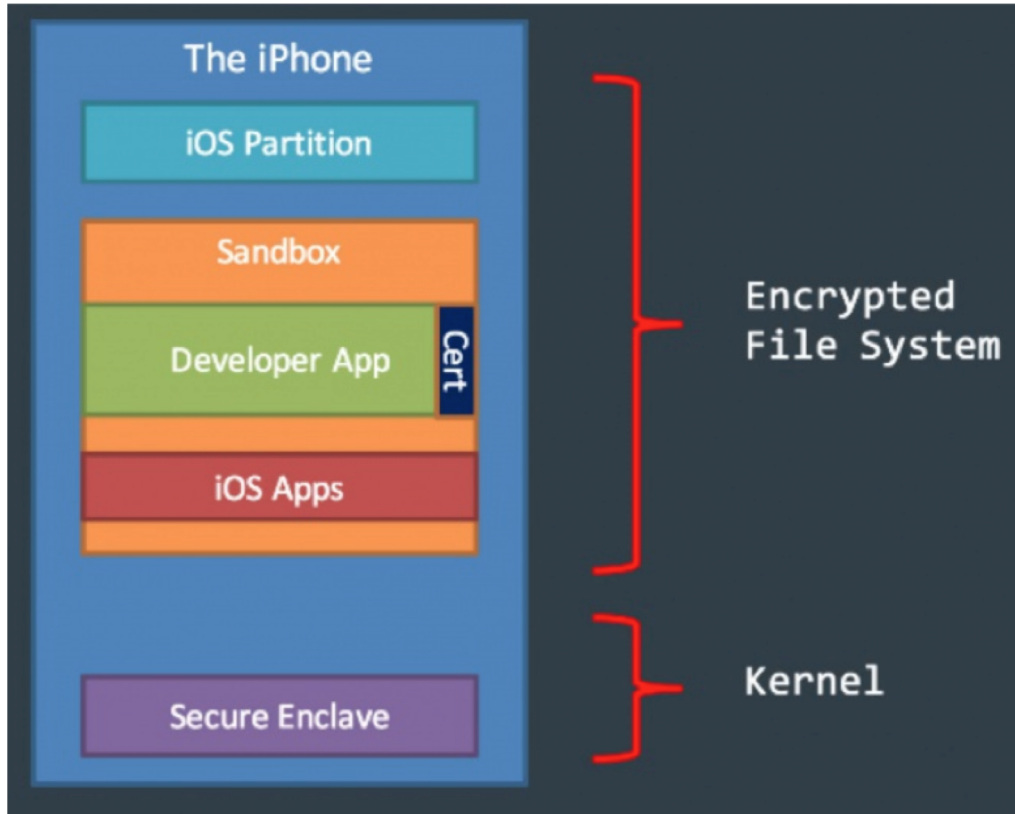
- ▶ Introducción
- ▶ Conocimientos previos
- ▶ Estudio de mercados alternativos
- ▶ Sistema de análisis y comparación
- ▶ Experimentación y validación
- ▶ Trabajo relacionado
- ▶ Conclusión y trabajo futuro

Introducción

- ▶ iOS es el sistema operativo móvil desarrollado por Apple
- ▶ Apple impone restricciones tanto a nivel de sistema operativo como en la publicación en su tienda de aplicaciones
 - ▶ Censura de diferentes temas dentro del App Store (violencia, xenofobia, racismo, etc)
 - ▶ Evita la presencia de aplicaciones maliciosas
- ▶ Surgimiento de mercados de aplicaciones alternativos al App Store

Conocimientos previos

iOS y su modelo de seguridad



- Hardware Security
 - Co-procesador Secure Enclave
- Secure Boot
 - Sistema de arranque firmado y distribuido por Apple
- Code Signing
 - Aplicaciones firmadas
- Sandbox
 - Permisos limitados
- Encryption and Data Protection
 - Datos cifrados
- Mitigaciones de Explotación de Código Nativo
 - ASLR
 - Bit NX

Conocimientos previos

Revisión de Aplicaciones en App Store



- Apple evalúa todas la aplicaciones y actualizaciones antes de publicarlas en el App Store
- Técnicas de evaluación no publicadas
- **Objetivo:** cumplir con la política y evitar código malicioso

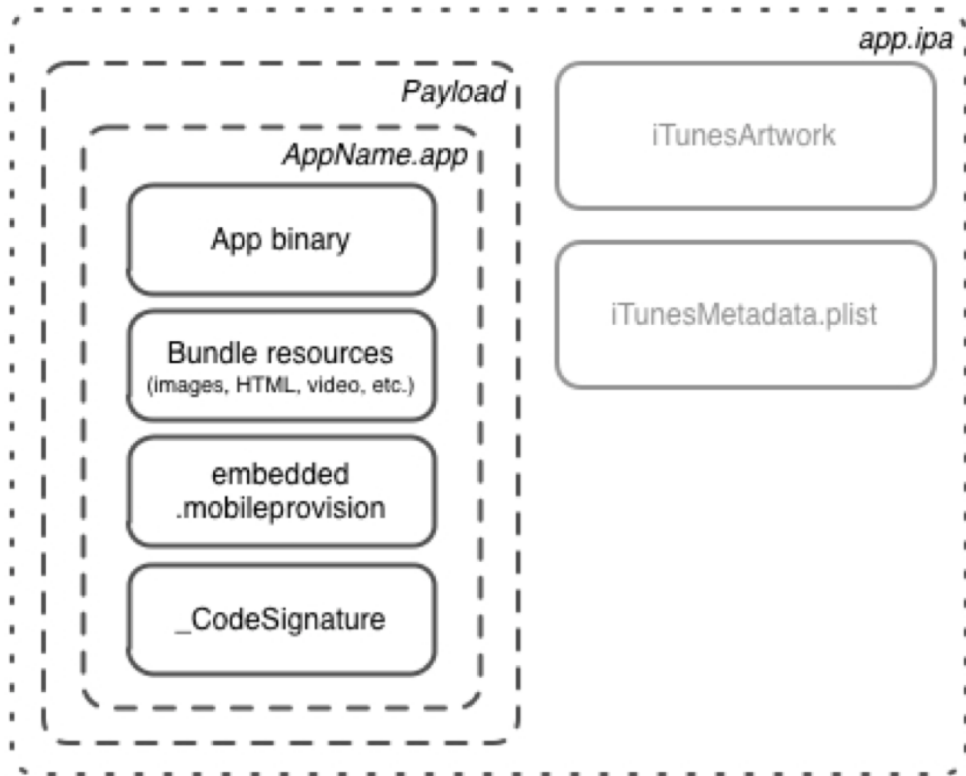
Conocimientos previos

Jailbreak

- ▶ Ataca la cadena de confianza establecida por Apple en el arranque del dispositivo
- ▶ Esto supone:
 - ▶ Deshabilitar los mecanismos de firma de código de iOS
 - ▶ Permitir que un dispositivo ejecute aplicaciones no aprobadas por Apple
 - ▶ Permitir instalar aplicaciones fuera de la sandbox que iOS implementa (lo que implica un mayor número de permisos para dichas apps)

Conocimientos previos

Aplicaciones iOS: formato IPA



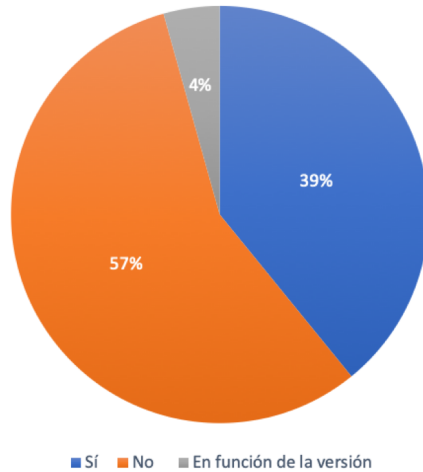
- **AppName.app/Info.plist:** Contiene la configuración de la aplicación
 - Permisos
 - Directivas de seguridad
- **AppName.app/App binary:** Contiene el código compilado de la aplicación
 - Cifrado si esta descargado del App Store

Estudio de mercados alternativos

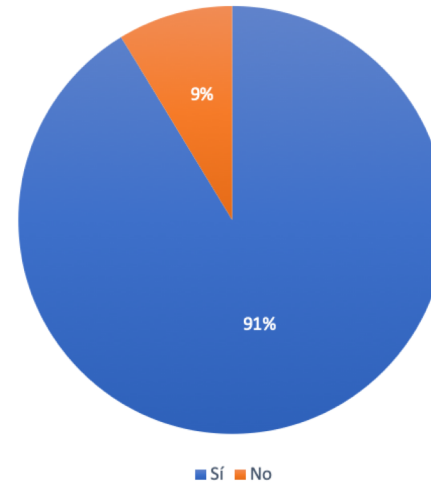
- ▶ Se ha realizado un estudio de 23 mercados alternativos al App Store que ofrecen aplicaciones para iOS
- ▶ Criterios para la comparativa:
 - ▶ ¿Requiere jailbreak?
 - ▶ ¿Contiene réplicas de aplicaciones publicadas en el App Store?
 - ▶ ¿Requiere registro?
 - ▶ ¿Es gratuito?

Estudio de mercados alternativos

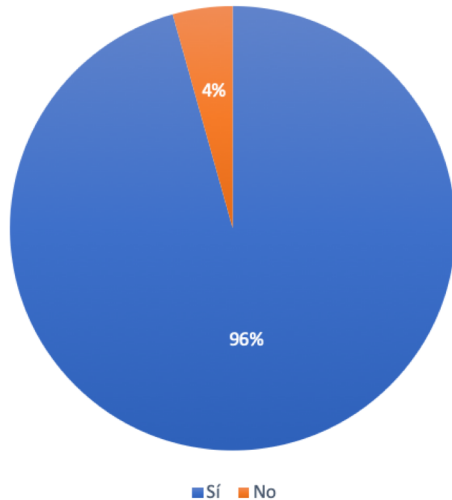
¿Requiere jailbreak?



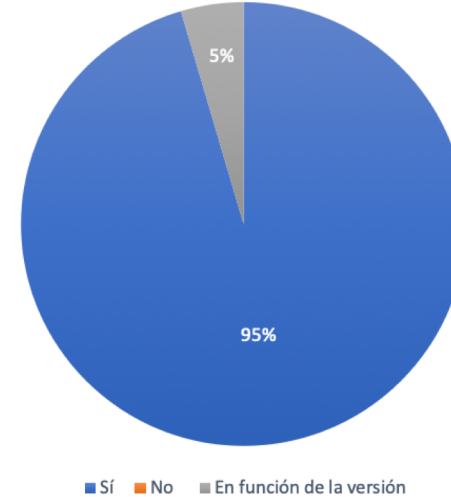
¿Requiere registro?



¿Contiene réplicas de aplicaciones publicadas en el App Store?

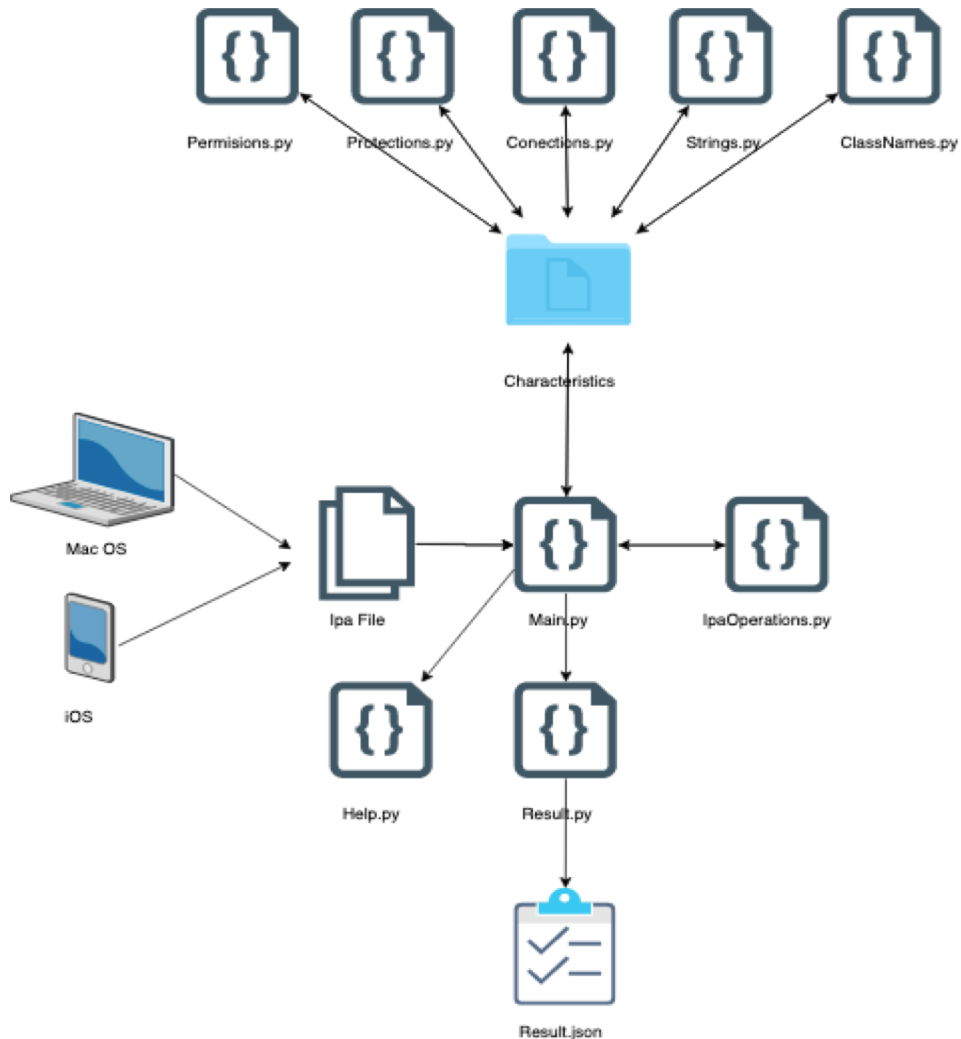


¿Es gratuito?



Nombre	Requiere Jailbreak	Contiene réplicas App Store gratuitas	Requiere registro	Es gratuito
Tuto App	No	Sí	En función de la versión	En función de la versión
VShare	No	Sí	No	Sí
Zestia Extender	No	Sí	No	Sí
Apps4iPhone	Sí	Sí	No	Sí
AppValley	No	Sí	No	Sí
Tweakbox	No	Sí	No	Sí
Appcake	Sí	Sí	No	Sí
51ipa	Sí	Sí	No	Sí
25 pp	Sí	Sí	No	Sí
Tongbu	Sí	Sí	Sí	Sí
App 704	No	No	Sí	Sí
Mojo installer	Sí	Sí	No	Sí
Ipa Box	No	Sí	No	Sí
App China	No	Sí	No	Sí
AppEven	No	Sí	No	Sí
HipStore	Sí	Sí	No	Sí
TopStore	No	Sí	No	Sí
iNoJB	No	Sí	No	Sí
Emus4U	No	Sí	No	Sí
IpaStore	En función de la versión	Sí	No	En función de la versión
Lee890	Sí	Sí	No	Sí
Asterix installer	No	Sí	No	Sí
Taigone Tikiri	Sí	Sí	No	Sí

Sistema de análisis



- Análisis estático de aplicaciones iOS
- Python 3
- Escalable
- Compatible con iOS y macOS
- Semi-automático

Sistema de análisis

Caso de uso: Spotify

▼ SpotifyAppStore:
▼ Statistics:
Permissions: 7
Connections: 139
Class: 6164
All Strings: 154767

▼ SpotifyAppStore:
► Statistics: {...}
▼ Protections:
canary: "true"
crypto: "false"
nx: "false"

▼ SpotifyAppStore:
► Statistics: {...}
► Protections: {...}
▼ Permissions:
0: "NSCameraUsageDescription"
1: "NSBluetoothPeripheralUsageDescription"
2: "NSPhotoLibraryAddUsageDescription"
3: "NSAppleMusicUsageDescription"
4: "NSMicrophoneUsageDescription"
5: "NSFaceIDUsageDescription"
6: "NSPhotoLibraryUsageDescription"

Caso de uso: Spotify

```

▼ SpotifyAppStore:
  ▶ Statistics:      {...}
  ▶ Protections:    {...}
  ▶ Permissions:    {...}
  ▶ Connections:    {...}

▼ Class Names:
0:      "SPTRemoteAccessoryCategorizer"
1:      "SPTAccessoryManagerLogging"
2:      "SPTAccessoryStateManagerImplementation"
3:      "SPTAccessoryManagerSessionServiceImplementation"
4:      "SPTAccessoryEndStreamTracker"
5:      "SPTAccessoryManagerAppServiceImplementation"
6:      "SPTAccessoryConnection"
7:      "SPTAccessoryDetector"
8:      "SPTAccessory"
9:      "SPTAccountSettingsCellFactory"
10:     "SPTAccountController7DayTrialProductActivation"
11:     "SPTAccountProductStateManagerController"
12:     "SPTAccountExternalLinkController"
13:     "SPTAccountControllerProductActivation"
14:     "SPTAccountControllerBuyPremiumActivation"
15:     "SPTAccountProductActivationUserFeedbackController"
▼ 16:   "SPTAccountProductActivationControllerImplementation"
17:   "SPTCampaignViewController"
18:   "SPTAccountSettingsViewModel"
19:   "SPTAccountPremiumInfoTableViewCell"
20:   "SPTAccountSettingsViewController"
21:   "SPTAccountPrepaidHelper"
22:   "SPTAccountCurrentProductMonitor"
23:   "SPTAccountServiceImplementation"
24:   "SPTAccountSettingsSection"
▼ 25:   "SPTAccountProductInformationControllerImplementation"

```

```

▼ SpotifyAppStore:
  ▶ Statistics: {...}
  ▶ Protections: {...}
  ▶ Permissions: {...}
  ▶ Connections: {...}
  ▶ Class Names: {...}
▼ Ipa Info:
  Bundle Identifier: "com.spotify.client"
  Ipa Version: "8.4.96"
  Minimum OS Version: "10.0"
  Allows Arbitrary Loads: "false"
▼ Network Exception Domains:
  0: "akamaihd.net"
  1: "scorecardresearch.com"
  2: "fbcdn.net"
  3: "facebook.com"
  4: "cdn.spotify.com"
▼ Application Queries Schemes:
  0: "comgooglemaps"
  1: "facebook-stories"
  2: "fb-messenger-share-api"
  3: "twitter"
  4: "fbshareextension"
  5: "fb-messenger"
  6: "fbapi20130214"
  7: "fbapi20130410"
  8: "fbapi20130702"

```

Sistema de comparación

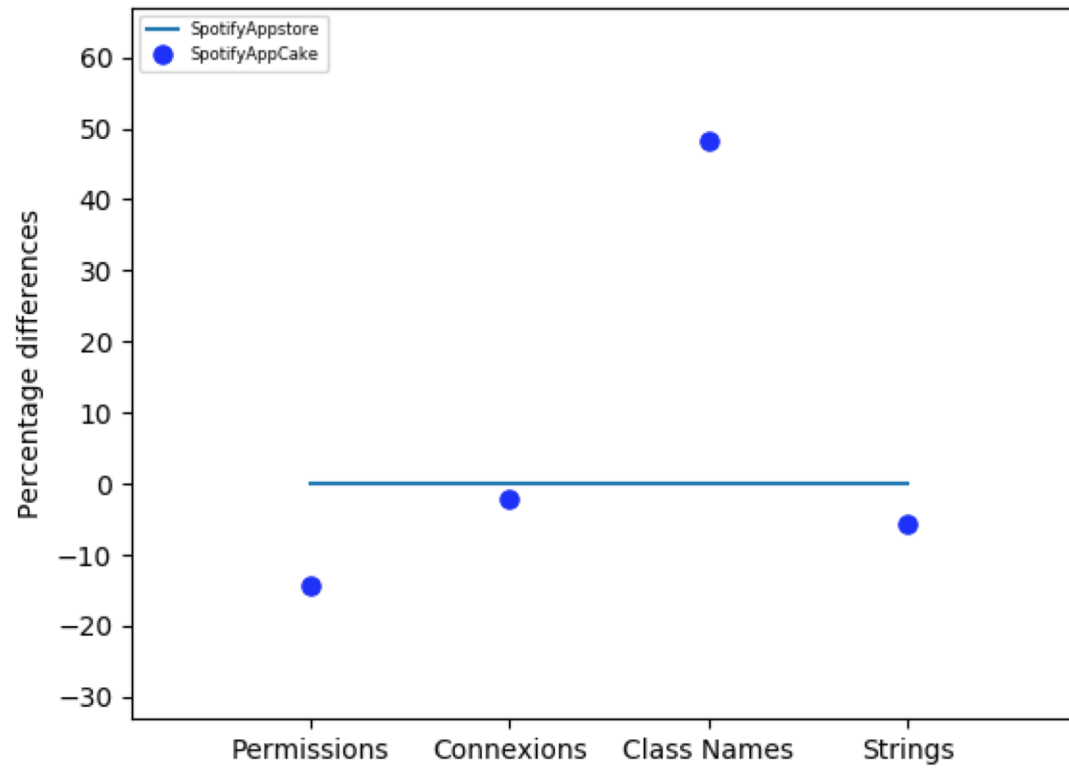
- Diferencias entre una aplicación descargada del mercado oficial de aplicaciones y las copias descargadas de mercados alternativos

▼ SpotifyAppStore_X_VS_Y_SpotifyAppCake:	
▶ Statistical differences (_Y_VS_X_):	{...}
Protections:	{}
▼ Permissions:	
0:	"NSMotionUsageDescription"
▶ Connections:	[...]
▶ Class Names:	[...]
▶ Ipa Info:	{...}
▶ All Strings:	[...]

▼ SpotifyAppStore_X_VS_Y_SpotifyAppCake:	
▶ Statistical differences (_Y_VS_X_):	{...}
Protections:	{}
▶ Permissions:	[...]
▶ Connections:	[...]
▶ Class Names:	[...]
▼ Ipa Info:	
Bundle Identifier:	"com.spotify.client"
Ipa Version Original APP_X:	"8.4.96"
Ipa Version Alternative APP_Y:	"8.4.3"
Minimum OS Version Original APP_X :	"10.0"
Minimum OS Version Alternative App_Y:	"8.0"
Allows Arbitrary Loads:	"false"
▶ Network Exception Domains:	[...]
▶ Application Queries Schemes:	[...]
▶ All Strings:	[...]

Sistema de comparación

Comparativa gráfica



Experimentos y validación

- ▶ Estudio inicial descartado debido a que AppEven no estaba disponible
- ▶ Estudio de 14 aplicaciones procedentes del App Store y de AppCake
- ▶ 7 aplicaciones de pago y 7 gratuitas
 - ▶ Las aplicaciones de pago estaban disponibles gratuitamente en AppCake
 - ▶ Versiones actualizadas en AppCake para las apps de pago
 - ▶ Versiones obsoletas en AppCake para las apps gratuitas

Experimentos y validación

Resultados

- ▶ De las 14 aplicaciones descargadas de AppCake, 9 incorporaban cifrado alternativo
 - ▶ El cifrado de estas aplicaciones no es el mismo que Apple utiliza en su mercado oficial

```
2PlayerQuizProAppStoreCifrado:
  Statistics: (...)
  Protections: (...)
  Permissions: {}
  Connections: {}
  Class Names: {}
  Ipa Info: (...)
  All Strings:
    0: "gy!$k"
    1: "5LPT,"
    2: "GLI/"
    3: "+c/TM!"
    4: "aiq("
    5: "zDQW"
    6: "s6RF0"
    7: "b>S0p>"
    8: "rY\u000c)"
    9: "dFu)"
    10: "R^%r"
    11: "Q=jN"
    12: "E0S="
    13: "o+gm"
    14: "hsc<"
    15: "2Gu)"
    16: " inu"
    17: "LRK|"
    18: "YVAL"
    19: "{y\"e%-a"
    20: "iUu,"
    21: "@}w7#"
    22: "\\\"y0"
    23: "\\Z'k"
    24: "bWw-"
    25: "3wM2"
```

```
2PlayerQuizProAppCake:
  Statistics: (...)
  Protections: (...)
  Permissions: {}
  Connections: (...)
  Class Names: (...)
  Ipa Info: (...)
  All Strings:
    0: "Matrix4x4f"
    1: "9Wk,"
    2: "Ch||"
    3: "6Sprite"
    4: "UnityPerMaterial"
    5: "Y+!>g"
    6: " ./Modules/ParticleSystem/ParticleSystem.h"
    7: "Error initializing outpu... and cannot be reused. "
    8: "j<7o"
    9: "hZH9"
    10: "Y4i%"
    11: "joystick 1 button 5"
    12: "-?[Sog"
    13: "SBY["a"
    14: "Flange depth. 0.01 to 1.0. Default = 1.0."
    15: "o6fh\\"
    16: "NhH'"
    17: "Transaction is nil"
    18: "kGL_ARB_texture_compression_bptc"
    19: "CaGa"
    20: "m_MuscleClipSize"
    21: "\u000cJpH!"
    22: "config"
    23: "HMAC-SHA-256"
    24: "updateRecord:inTableWithName:columnName:columnValue:error:"
    25: "gfx device initialization failed"
```


Experimentos y validación

Resultados

- ▶ 3 aplicaciones no han sufrido modificaciones (Infinity Flight, Vlc y Helix Dump)
- ▶ En la aplicación Pinterest, diferencias debidas a la disparidad de versiones entre la app perteneciente al App Store (7.28.1) y la app relativa a AppCake (6.59)
- ▶ La aplicación Pou perteneciente a AppCake realiza una conexión diferente a la de la App Store
 - ▶ Ha sido modificada para añadir un sistema de cobro por publicidad (Google Ads)

Nombre	Permisos	Conexiones	Clases	Strings
Pinterest (App Store)	8	88	3827	110133
Pinterest (AppCake)	8	113	7554	110660
Vlc (App Store)	3	97	3210	118588
Vlc (AppCake)	3	97	3210	118588
Infinity Flight (App Store)	2	2	187	19683
Infinity Flight (AppCake)	2	2	187	19683
Helix Dump (App Store)	5	138	3951	127312
Helix Dump (AppCake)	3	138	3951	127312
Pou (App Store)	7	27	2722	21395
Pou (AppCake)	7	27	2722	22759

```
▼ pouAppStore_X_VS_Y_PouAppCake:
  ▼ Statistical differences (_Y_VS_X_):
    Permissions: 0
    Connections: 0
    Class: 1361
    All Strings: 1364
    Protections: {}
    Permissions: []
  ▼ Connections:
    ▼ 0: "https://pagead2.gppglfszndjcbtjpn.cpm/pagead/gen_204"
```

```
▼ 172: "https://googleads.g.dpvblfcljck.nft/mads/static/mad/sdk/native/mraid/v2/mraid_app_expanded_banner.js"
```

Trabajo relacionado

- ▶ El análisis estático se realiza al código de una aplicación que no se encuentra en ejecución
 - ▶ Permite conocer todos los posibles caminos del código de la aplicación
- ▶ El análisis dinámico se realiza en tiempo de ejecución
 - ▶ Solo analiza el camino que el código toma en esa ejecución concreta
- ▶ Necesidad de utilizar análisis estático de aplicaciones iOS
 - ▶ El análisis dinámico solo cubre una parte pequeña del código
- ▶ Los análisis estáticos realizados hasta el momento cubrían
 - ▶ Llamadas a APIs privadas
 - ▶ Flujos de datos
- ▶ La mayoría de las muestras de malware analizadas se encuentran alojadas en mercados alternativos

Conclusión y trabajo futuro

- ▶ Gran parte de los mercados alternativos estudiados contienen réplicas de aplicaciones publicadas en el App Store. 13 de los 23 mercados no necesitan jailbreak
- ▶ Se ha desarrollado un sistema de análisis estático y comparación para obtener características de forma semi-automática
 - ▶ Semi-automática ya que requiere de un IPA con el binario descifrado
- ▶ De las 14 aplicaciones estudiadas, tan solo 4 no habían sido modificadas
 - ▶ Una de ellas implementa un sistema de cobro por publicidad

Conclusión y trabajo futuro

▶ Trabajo futuro:

- ▶ Añadir los métodos que implementan las clases
- ▶ Añadir análisis dinámico de aplicaciones iOS al comparador y analizador
- ▶ Ampliar el número de mercados alternativos analizados
- ▶ Analizar y descifrar la capa de seguridad añadida por AppCake
- ▶ Aumentar la compatibilidad dando soporte a sistemas operativos basados en Linux