03/06/2019

Sistemas Ubicuos - Introducción

Àlex Soler

AttackIQ

Frida and Radare2 Fanboy (herramientas de reversing para móvil)

* Taller de Frida dará en ¿setiembre?

4 prácticas en 3 semanas

* Guiadas
* Hacking sencillo
* Emuladores (máquina virtual MacOS para ios y también en Android)
* Pequeño informe después de cada práctica (screenshots)
  + Qué se ha hecho y porqué
  + Y algunas preguntas añadidas
* Entrega en PDF, nombres tanto en el interior como en el nombre del fichero
* 1 punto en clase
* X en laboratorio
* X en examen

**IOS**

Dylib – llibreires del kernel de Darwin/CoreOS – basat en uNIX

* auditoria de iphones, mejor tener un iphone (5S-60€ en adelante) iphone 6 uns 100-150€ Ualapop. A partir del 8S, p.e., emprenta dactilar

ARM – tipus d’arquitectura (com ara x86 en intel)

Llegir link on hi ha més información <https://www.apple.com/business/docs/iOS_Security_Guide.pdf>

Secure Enclave – coprocesador per gsetionar els ciffratges. Introudït en el moment que s’utilitza l’empremta dactilar (com a dada biométrica)

Application Sandbox – cada aplicación s’executa a la seva propia carpeta.

A la que alliberem un móvil (jailbreak) .. totes aquests temes de seguretat deixen de tenir sentit (usuari root)

Keychain – base de dades de passwords

Ksec – segretat no sobre fitxers, sino sobre

Que quedi clar:

* no es permet fer downgrade de versions de iOS. Qualsevol aplicación que ho permeti, és malware.

JAILBREAK

* Entendre bé, Tethered i Untethered

<https://www.theiphonewiki.com/wiki/jailbreak>

si volem comprar en ualapop un iphoen 5, pe..e, aquesta web va bé per saber quins models I versions són susceptibles de fer jailbreak

Cydia Impactor

Té un problema: applicació de 3ers.. i necesita password de itunes

Node –applesign (conte nowsecure de github)

¡!! Crear cuenta de itunes para hacer las prácticas:

País de origen: Suiza

4/6/2019

Instal·lar Unc0ver o Electra com a jailbreak. Són fitxer ipa.

En Apple ID generamos un password para instalar el ipa desde Cydia impactor (hace todo lo que veremos aahora, de manera desatendida)

Recordemos que con la herramienta node-applesign podemos instalar una aplicación sin necesidad de la credencial/certificado de Apple-id. El certificado que usamos lo autogeneramos, y Apple lo acepta.

Node bin/applesign.js –m ../jb\_11.2.2/ … -I ….

Mobileprovision, tambien es necesario para ejecutar aplicaciones.

Tanto el certificado “local” como el mobileprovision se generan en la primera instalacio´n

De momento sólo estamos haciendo cosas en el mac…. No en el móvil, pq aún no tenemos el jailbreak, no podemos instalar nada.

¡!instalar XCode!!!

Con la primera aplicaci´n instalada (aunque esté vacia), genera el certificado y el mobileprovision que necesitaremos

Despueés de hacer un jailbreak, se autoinstal.la el Cydia que es como un repositorio para guardar apps.

Todo lo que instale quedarà en el equipo, pero cuando reinicie.. no se ejecutaran pq entraremos con otro usuario

Por eso SemiTethering

Password por defecto ssh – alpine – CAMBIARLO al primer acceso

Usbmux – libreira para acceso remoto

github del profe alex soler – trobarem scripts de python

recordemos que una aplicación sólo puede guardar en su carpeta

Grupo 1

IP: 185.209.212.36

Computer name: xcloud432

Username: Xcloud

Password: 9xW3bJLb - GTeam

Steps

* Connexio VNC
* Configure ssh – hablitem des del sharing: remote login
* Install xcode – amb el apple id que hem creat

Tricks de Xcode

* Create a new project
* Single app .
  + posar nom
  + ruta
* tenim molts simuladors de diferents iOS
  + agafar entre un 5S i un 6
* fer “play”
  + tindrem un iphone simulat i és on farem les pràctiques

Auditorias para móviles:

OWASP Mobile Security Testing Guide – Github, p.e

Analisis estatico – analiza aplicación sin ejecutar

Analisis dinamico – ejecuto la aplicación y veo qué es lo que hace. Hooking (intercepció)

Almacenaje de datos inseguro

1. Aplicación en si ya es un punto de ataque.
2. Almacenaje local . insecure data storage. 2º punto que veremos sobre las superficies de atque a un mobil
3. Comunicaciones

SQLite

* Siempre es inseguro trabajar con este tipo de base de datos
* Además, los ficheros(¿) empiezan siempre con Z

UIPasteboard

* Cuidado , pq pueden haber buffers (copia/pega) que se compartan entre varias aplicaciones ( y si hay un malware escuchando ese buffer… y copiamos un password, …)
* Soluciones… borrar, pe.e el pasteboard si la aplicación entra en segundo plano

Contenedor

* Teniendo jailbreak… se podrían leer toda la infronació que se guarde en texto plano en el móvil

Aplicación:

* No guardes información
* Si la guardas, cifrada almenos

---pracitcas voluntarias: jailbreak de un mobil, jugar con alguna aplicación averiguar qué hace con datos, almacenaje, base de datos, logs, etc…

Burb- para proxear. Si queremos además ver las comunicaciones https, tendremos que instal.lar el certificado de burb en el móvil.

Certificate Pinning

Hardcodear en mi aplicación parte del certificado de mi servidor. La aplicación sólo confía en sus certificados

Se puede bypassear con SSL Kill Switch (teniendo jailbreak)

Preguntas final clase: kahoot

* Donde se puede almacenar información sensible?
* Qué son los Core services y cómo almacenan la información

11/06/2019

Dimarts..

Ahir dilluns, no va haver-hi clase per ser festiu, i la recuperarem el proper dijous

* seguridad en iOS – 3 -

part dura de teoría (s’acosta molt a l’engineria inversa – reversing) per tal d’estudiar la lógica de l’aplicació.

* Complicat análisis estàtic, corva d’aprenentatge lent
* El que farem és més aviat análisis dinàmic… hi ha eines que aporten comoditat

Objective-C – llenguatge orientat a missatges

Analitzant les seccions del segment TEXT, podrem fer l’analisis de reversing (noms de mètodes, noms de clases, etc…)

Load Commands

Nos interesará 1. Recordem que els binaris están xifrats, el Mach-O, concretament. I se xifra tant el codi com les seccions..

I una aplicación es desxifra cada vegada que s’ha d’executar en memoria. Hi ha un load command que ens dóna aquesta información (eina o-otool)

Cryptoff – offset a on comença el xifrat

Cryptsize – tamany del paquet xifrat

…

Eïna Otool

Permet coneixer totes les llibreries lincades dins l’aplicació.

ASLR

Permet executar l’aplicació en diferents espais de memoria cada vegada q s’executa… per temes de seguretat, és millor, ja q no és previsible.

Si el binari s’ha compliat amb PIE, es podrá desxifrar, tindrà ASLR.

La <baseAddr> será diferent cada vegada si està feta amb PIE.

La <baseAddr> será sempre la mateixa en cas q l’aplicació no estigui compiada amb PIE

¡! Nmoés desencriptar el codi… no el header, p.e.,

¡!tenir clar el procés!! Els 6 punts, p.e.

Pq hi ha aplicacions que facilien la feina:

* Clutch – iOS11
* BFDecript – iOS12 PLZ

Cycript

Avui en dia, és poc utilitzat

FRIDA

És el més usat actualmente.

Té un motor de javascript

AVIS PRàctica:

Creació handler des del directori Frida-trace.

Al executar altra vegada des del mateix directori… i utilitza els mateixos fiters.

De manera que creariem directoris.. anidats…

¡posar-li complicat al profe : p.e., no buscar codis públics

DEBUGING..

Ja és a molt baix nivell, no entrarà.

**Preguntes:**

Fer-li ullades a les preguntes que posa a les transparències.

PRACTICA

Dins el móvil hi ha dues carpetes importants de conèixer:

* Bundle . inclorà el paquet del binari
* Data. Información q almacena aplicación (p.e. per buscar información senseible que guarda l’aplicació)
* Shared

Deviceset.plist

Directori dels tipus de iphone. El conteidor de l’aplicació, tinguem en compte que estarà dins del directori de l’iphone corresponent que estem utilitzant:

Iphone-6 ->52ABE…etc

I com saber per trovar l’aplicació:

Find . | grep –i dynamicanalsys

JAILBREAK Detection

Tots els jailbreaks deixen rstres… fitxers… i el que farem será buscar un d’aquests fitxers.

A la pràctica hoockegem aquest mèotde, i al fer login, buscarem les crides al mètode.

Tenim un codi per convertir un codi a string per saber què s’està hoockejant…

Si existeix: TRUE

¡!!cada vegada que fem un login, haurem d’executar l’script de bypass del jailbreak

Developer.apple.com

Aquí podem trovar descripcions dels diferentes metodes d’objective C

Practica classdump:

Ens fa falta el binari… i el trobarem dins de Bundle (dins de la carpeta DynamicAnalysis.app)

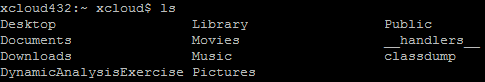
class-dump DynamicAnalysis

a la pràcitca, ens proporcionen el binari ja desxifrats.

Objective C

El “-“ mètode de instancia?

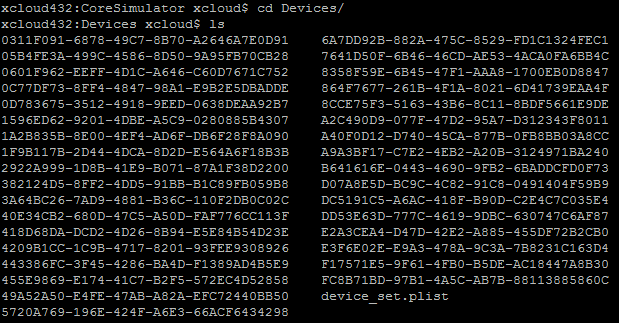
El “+” mètode de classe?



Per trovar la carpeta Bundle:

xcloud432:~ xcloud$ **find . | grep Bundle**

La que ens interessa està a /Library/Developer/CoreSimulator/Devices



Dins el fitxer device\_set.plist, podem veure a quin codi correspon l’Iphone 6S que hem triat:



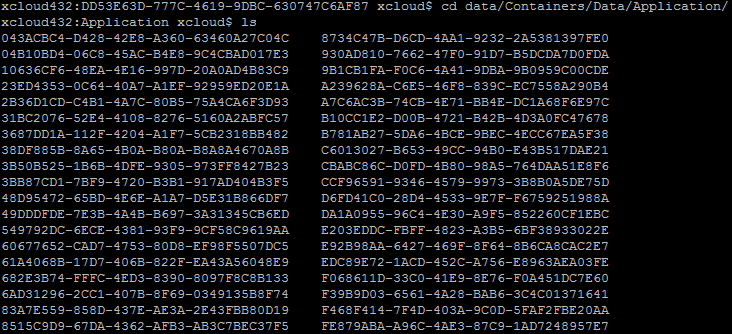
Busquem la carpeta DD53E63D-777C-4619-9DBC-630747C6AF87 i cerquem dins el seu Bundle i Data directoris



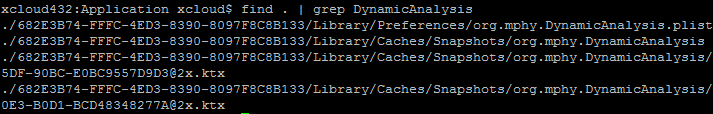


L’aplicació està dins de:





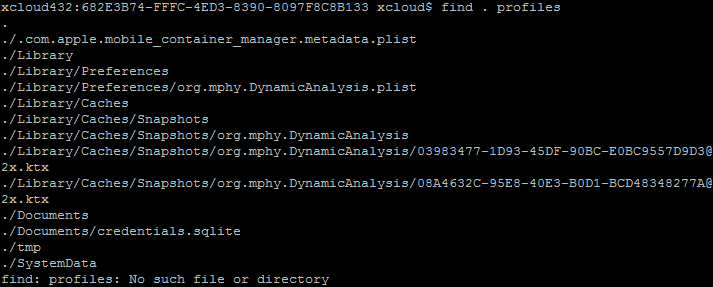
I fem una recerca del nom de l’aplicació dins aquests directoris:



Hem de fer un DUMP de les clases. (no hi ha classdump per a Linux – millor fer-ho amb radare)

-amd radare : r2 … icc

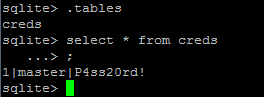
Per buscar les credencials fem una recerca del texte “profiles” dins els directoris de l’aplicació:



Ens crida l’atenció la base de dades “credentials.sqlite” així que hi entrem:

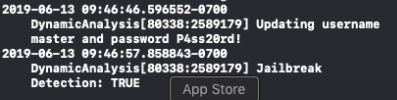


Llistem les taules disponibles i n’obtenim una: “creds”

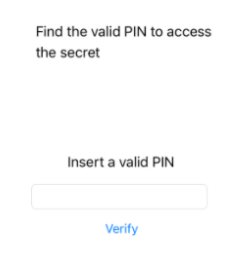


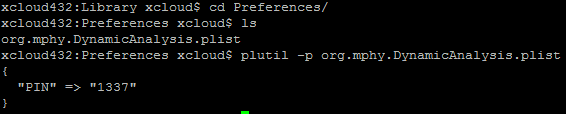
Fent una select, podem llegar directament les credencials del LOGIN

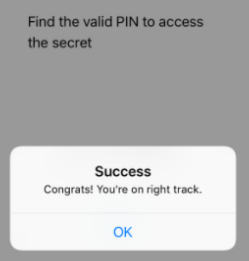
Adonem-nos que les credencials les podem veure en text pla a la finestra de Xcode on es veu el progres de l’execució de l’aplicació.



Una altra cosa que haurem d’esbrinar quan entrem el login/pass a l’aplicació, és un PIN:





o **Dónde se almacenan las credenciales del usuario y en qué formato? Se almacenan**

**de dos formas distintas.**

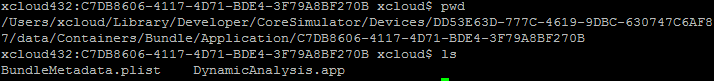
o **Dónde se almacena el PIN y en qué formato?**

o **Indica los comandos/herramientas empleados para acceder a la información**

**almacenada.**

o **¿Cómo deberían almacenarse estas credenciales y el PIN de forma segura?**

Trobem la ubicació del binari



i en fem un classdump

/Users/xcloud/Library/Developer/CoreSimulator/Devices/DD53E63D-777C-4619-9DBC-630747C6AF87/data/Containers/Bundle/Application/C7DB8606-4117-4D71-BDE4-3F79A8BF270B/DynamicAnalysis