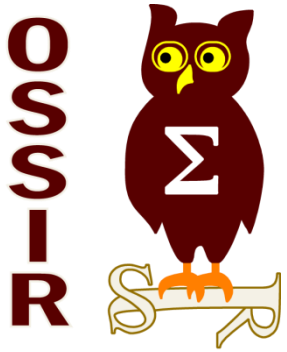
14 avril 2015



Rooted Con 2015 : Compte-rendu

OSSIR 14/04/2015

solucom
management & IT consulting

Rooted Con

- LA conférence *infosec* en Espagne 
  - Fondée par Roman Ramirez
  - 6ème édition cette année
- A Madrid, les 5/6/7 mars 2015
  - Hôtel Auditorium
- 1000+ personnes présentes cette année
- 24 conférences

Le programme de ce compte-rendu

- Focus sur 5 conférences marquantes…

THURSDAY, MARCH 5th 2015	
10:00 – 10:30	Rooted CON staff Keynote
10:30 – 11:30	Infección en BIOS, UEFI y derivados: desde el mito a la realidad David Barroso
11:30 – 12:00	BREAK/CALL FOR RESEARCH
12:00 – 13:00	LECr* elviervice Pack 2 (* Ley de Enjuiciamiento Criminal, Criminal Procedure Act) Jorge Bemúdez
13:00 – 14:00	Bug Bounties 101 Christian Lopez
14:00 – 15:30	LUNCH
15:30 – 16:30	Andrzej Dereszowski Turla:Development & Operations – the bigger picture
16:30 – 17:00	How I met your eWallet Yaiza Rubio y Felix Brezo
17:00 – 17:30	BREAK/CALL FOR RESEARCH
17:30 – 19:00	Rooted Panel I – Does someone have to give a hacker license?
19:00 – 19:15	*Rooted CON 2015 Day 1 closure*

FRIDAY, MARCH 6th 2015	
10:00 – 11:00	Finding stegomalware in an ocean of apps… Alfonso Muñoz y Antonio Guzman
11:00 – 11:30	Investigando sobre los cortafuegos de aplicaciones web Carmen Torrano
11:30 – 12:00	BREAK/CALL FOR RESEARCH
12:00 – 12:30	WEBEX: Análisis de datos en bruto Abel Valero
12:30 – 13:00	Deep inside the Java framework Apache Struts (Str-SUCK-ts) Julian Vilas
13:00 – 14:00	On Relaying NFC Payment Transactions using Android devices Ricardo J. Rodríguez y José Vila
14:00 – 15:30	LUNCH
15:30 – 16:30	Desmitificando Apple Pay Sebastian Guerrero
16:30 – 17:30	Rojos y Azules: dos equipos con dos sabores Alejandro Ramos
17:30 – 18:00	BREAK/CALL FOR RESEARCH
18:00 – 19:00	El tiempo en MIS manos Jose Selvi
19:00 – 20:00	Ingeniería inversa de circuitos integrados Eduardo Cruz
20:00 – 20:15	*Rooted CON 2015 Day 2 closure*

SATURDAY, MARCH 7th 2015	
10:00 – 11:00	Bend the developers to your will Miguel Tarasco
11:00 – 11:30	(in)seguridad en el gran casino Pablo Casais
11:30 – 12:00	BREAK/CALL FOR RESEARCH
12:00 – 13:00	Ampliando el arsenal de ataque Wi-Fi David Perez y José Picó
13:00 – 14:00	Y por último, pero no por ello menos importante… Hugo Teso
14:00 – 15:30	LUNCH
15:30 – 16:30	Physical Penetration Testing Eduardo Arriols
16:30 – 17:30	Can I play with madness Chema Alonso
17:30 – 18:00	BREAK/CALL FOR RESEARCH
18:00 – 19:00	Android: Back to the Future (Too? or Two?) Raúl Siles
19:00 – 20:00	Bypassing DRM Protections at Content Delivery Networks Adrian Villa
20:00 – 20:15	*Rooted CON 2015 closure*

- … et résumé très bref de toutes les autres

J1 - Rooted Panel I – Does someone have to give a hacker license?

- **Table ronde** sur un sujet visiblement **très controversé** en ce moment en Espagne : **la réglementation du marché privé de la sécurité de l'information**
- **Loi pénale en cours de préparation** visant à requérir une accréditation spécifique, un **"permis hacker"**, pour toute personne souhaitant en **faire son métier**
- **Projet de loi actuellement très flou,** de nombreuses questions sans réponses :
  - Qui des **individus ou des entreprises** va être concerné par cette loi ?
  - Dans le cas d'individus, **toute personne** manifestant un intérêt pour la SSI va devoir s'enregistrer ?
  - D'ailleurs, ce **permis va être payant** ? Qui va le financer ?

J1 - Rooted Panel I – Does someone have to give a hacker license?

- Nageant dans ce flou, les **thèmes suivants** ont été abordés :
  - Comment reconnaitre les **talents** ?
  - Quelles **qualités** doit avoir un hacker ?
  - Est-ce qu'un **outil tel que nmap** est ou va être **considéré comme une cyberarme** selon cette nouvelle loi pénale ?
  - Pourquoi n'existe-t-il **pas de formation universitaire** dans le domaine de la sécurité de l'information ?
  - Est-ce que les **attaquants sont aussi de bons défenseurs** ?

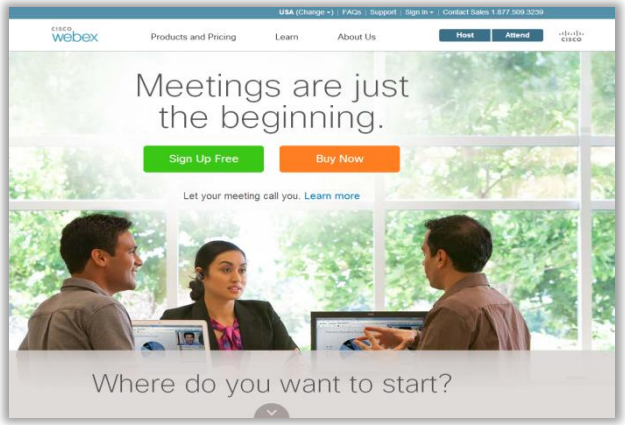
- En **conclusion**, le **phénomène de la « fuite des cerveaux »** vers des pays plus attractifs et offrant plus d'opportunités aux chercheurs de sécurité, tels les **États-Unis**, a été évoqué **comme pouvant être accru avec ce projet de loi**

Pour résumer

- Prise de conscience au niveau de **l'état espagnol des enjeux de la SSI**
- Volonté de **réglementer le marché**
- **Contours très flous** du projet de loi

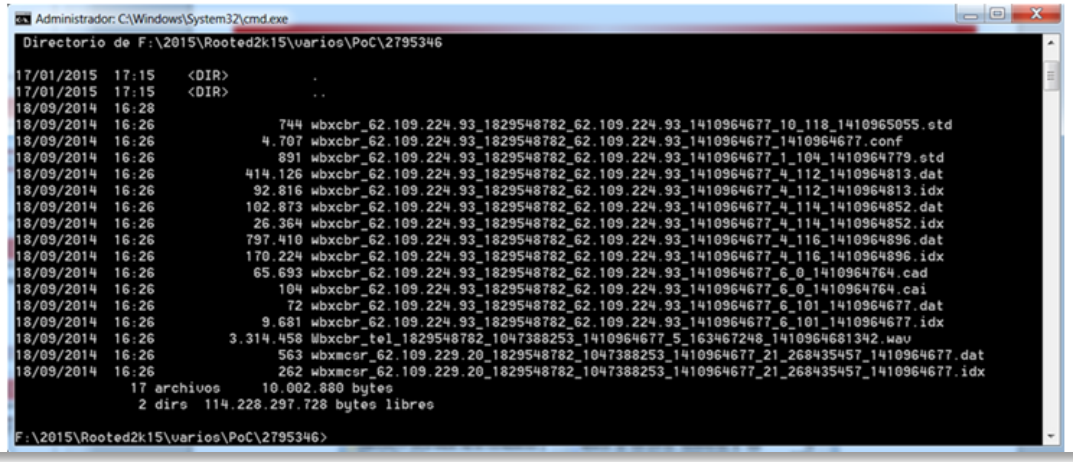
J2 - WebEx : analyse de données brutes – Abel Valero

- **Problématique :** Abel Valero **perd accidentellement le support PowerPoint** d'une formation qu'il avait **dispensé via Cisco WebEx** quelques temps auparavant et qu'il avait rendu **« non-téléchargeable » par les options proposées par WebEx**
- **Motivation :** tenter de **récupérer l'enregistrement vidéo** de la formation WebEx
- **Solution :** recouvrir le **format vidéo propriétaire** à partir des **fichiers temporaires** téléchargés lors du visionnage du contenu



Recuperación de archivos

Gracias a un archivo con extensión ".wav" pude determinar que esta era mi conferencia



Análisis en bruto

Marca "WAV" dentro de los datos en bruto

```
# 3 [0x0-0x98a548]
hits: 0
[0x00000000]> / "rif"
Searching 5 bytes from 0x00000000 to 0x0098a548: 22 72 69 66 22
# 3 [0x0-0x98a548]
hits: 0
[0x00000000]> / "WAV"
Searching 5 bytes from 0x00000000 to 0x0098a548: 22 57 41 56 22
# 3 [0x0-0x98a548]
hits: 0
[0x00000000]> / WAV
Searching 3 bytes from 0x00000000 to 0x0098a548: 57 41 56
# 3 [0x0-0x98a548]
hits: 1
0x00189534 hit0_0 "WAV"
[0x00000000]> s hit_0_0
[0x00000000]> px 80@0x00189534
- offset -   0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF
0x00189534  5741 5645 666d 7420 1200 0000 0700 0100  WAVEfmt .......
0x00189544  401f 0000 401f 0000 0100 0800 0000 6661  @...@.........fa
0x00189554  6374 0400 0000 f66b 0100 6461 7461 e092  ct.....k..data..
0x00189564  3200 ffff ffff ffff ffff ffff ffff ffff  2...............
0x00189574  ffff ffff ffff ffff ffff ffff ffff ffff  ................
[0x00000000]>
```

J2 - WebEx : analyse de données brutes – Abel Valero

Análisis en bruto

Visualizando en 32bits se puede ver de forma mas clara los valores.

E incluso distinguir lo que podrían ser: Identificadores, offsets ....

```
0x00000010  0x0000001b 0x00000000 0x00070100 0x00000000  ................
0x00000020  0x0000037b 0x00000000 0x00000378 0x00000000  {.......x.......
0x00000030  0x00000000 0x00000000 0x00070103 0x00000000  ................
0x00000040  0x000002e8 0x00000000 0x000006f4 0x00000000  ................
0x00000050  0x00000000 0x00000000 0x00070112 0x00000000  ................
```

.... y tamaños:

```
0x00000010  0x0000001b 0x00000000 0x00070100 0x00000000  ................
0x00000020  0x0000037b 0x00000000 0x00000378 0x00000000  {.......x.......
0x00000030  0x00000000 0x00000000 0x00070103 0x00000000  ................
0x00000040  0x000002e8 0x00000000 0x000006f4 0x00000000  ................
```

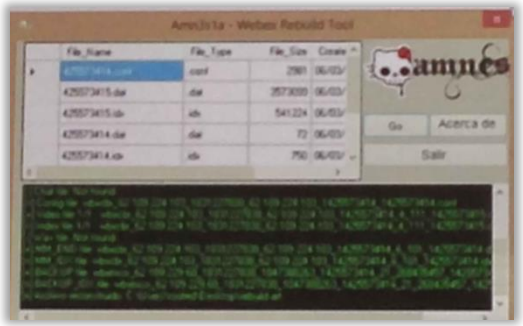
Secciones (Items)

```
ARRAY[0 to Numero Secciones]
18-1b = ID Tipo Bloque                  DWORD 4-bytes
1c-1f = Indice Bloque *                 DWORD 4-Bytes
20-23 = Tamaño Bloque                   DWORD 4-bytes
24-27 = NULL                            DWORD 4-bytes
28-2b = Offset Bloque en el archivo     DWORD 4-bytes
2c-2f = null                            DWORD 4-bytes
30-33 = null                            DWORD 4-bytes
34-37 = null                            DWORD 4-bytes
```

IDS	Tipo	Archivo/Extension
70100	chat	"_1_.std"
70103	file	"_10_.std"
70112	conf	".conf"
7010c	video	"_4_.dat"
7010d	video idx	"_4_.idx"
70105	sonido	"_5_.wav"
70114	finV	"_6_.dat"
70115	quick/desc	"_6_.idx"
7010A		"_6_.cad"
7010B		"_6_.cai"
70110	backup	"_21_.dat"
70111	base64	"_21_.idx"

- **Difficultés :** quasi-aucune
  - **Pas de chiffrement, ni obfuscation du format**
  - Néanmoins quelques **hypothèses** à faire en début d'analyse…
  - …et quelques zones dont la **fonction** n'a pas été identifiée (champs optionnels etc.)

PoC via un outil de reconstruction automatique : l'auteur souhaite le rendre public…une fois Cisco informé



Pour résumer

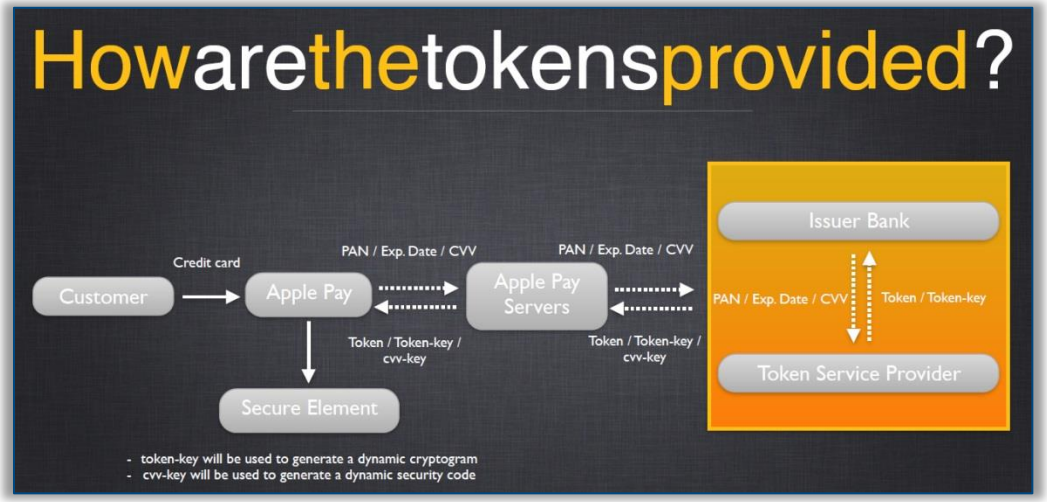
- **Exercice intéressant** de reconstruction de format
- **Impact conséquent, permettant le contournement des protections de contenu**

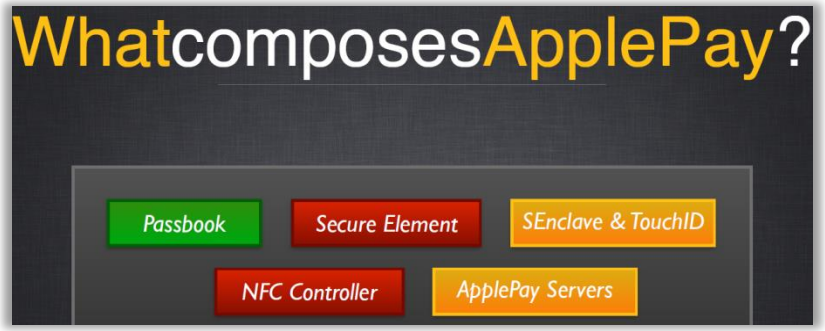
J2 - Demystifying Apple "Pie" & TouchID – Sebastian Guerrero

- **Objectifs :** Détailler le fonctionnement technique et les vulnérabilités du système de **paiement mobile Apple Pay** et du système de **reconnaissance par empreinte digitale TouchID**

- **En préambule, par l'auteur :**
  - **Travaux** de recherches de vulnérabilité toujours **en cours**
  - Vulnérabilités présentées requièrent toutes que le **terminal soit jailbreaké**
  - **Aucun 0-day** diffusé dans la présentation

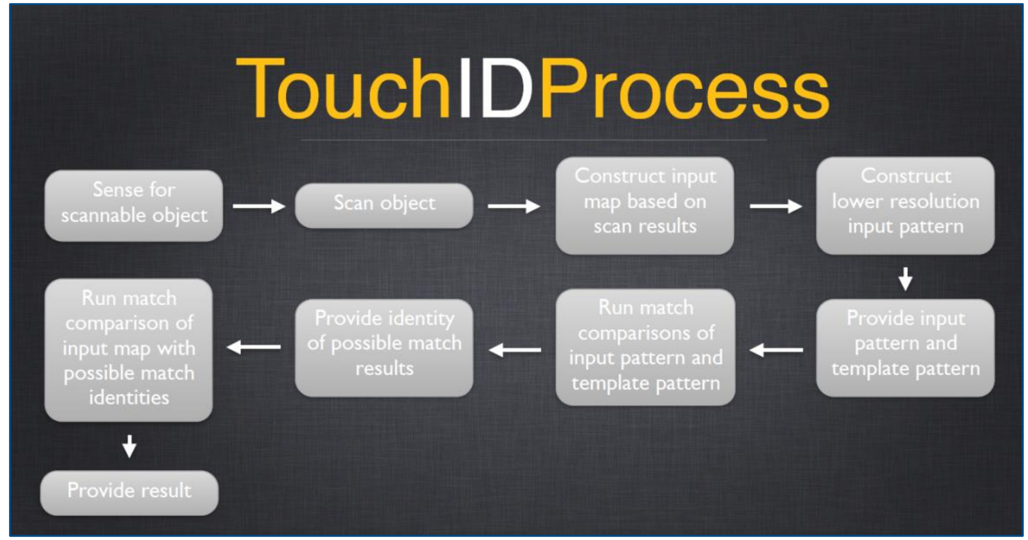
- **Apple Pay :**
  - Le ***Secure Element*** contient un **token pour chaque carte de crédit** enregistrée par l'application PassBook
  - Un **token** correspond à une **valeur anonymisée d'une CB**
  - Ce token est **émis par un service Web d'Apple**



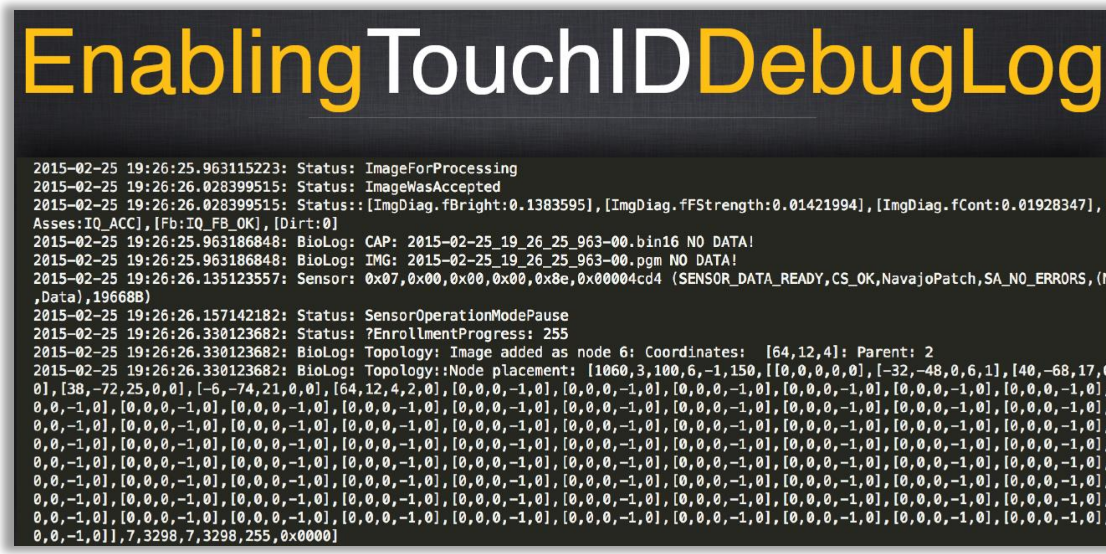


J2 - Demystifying Apple "Pie" & TouchID – Sebastian Guerrero

- **Apple TouchID :**
  - Le composant ***Secure Enclave*** (SEnclave) est utilisé pour stocker les empreintes
  - Le SEnclave correspond concrètement à une **mémoire Flash de 4 Mo qui dispose de son propre processeur, de son propre OS (SEP OS)**
  - L'utilitaire **SEPUtil** assure les communications avec le SEnclave
  - Les données stockées au sein du SEnclave peuvent **uniquement être déchiffrées par une clé qui est contenue dans le Senclave**



- **Vulnérabilités :**
  - Existence d'une option (de développement?) ***DebugLog*** permettant **d'afficher les "noeuds" digitaux lié à une empreinte**

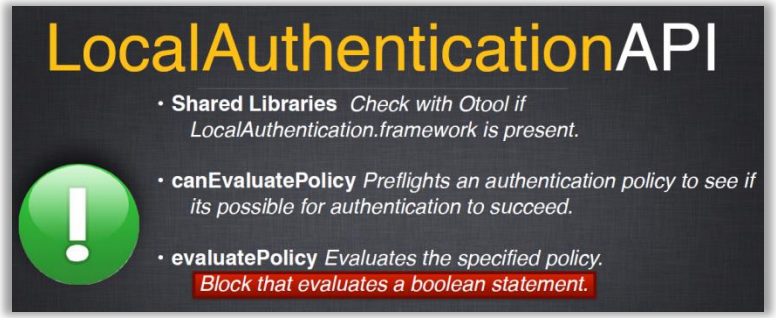


J2 - Demystifying Apple "Pie" & TouchID – Sebastian Guerrero

- **Comment faire appel à la vérification TouchID ? 2 API possibles**
  - Au niveau **système : *LocalAuthentication***
  - Ou **directement au niveau du *Secure Enclave : KeyChain***

- **Vulnérabilités :** possibilité de patcher *LocalAuthentication* (possible avec terminal jailbreaké) pour altérer le **résultat booléen d'une demande d'authentification**

PoC par l'auteur qui a pu déverrouiller son terminal…avec son nez



Pour résumer

- **Implémentation quasi conforme à ce qui a été annoncé**
- **Peu de vulnérabilités jusqu'ici, qui requièrent de toute façon un terminal jailbreaké**

J3 – (In)sécurité dans le grand casino – Pablo Casais

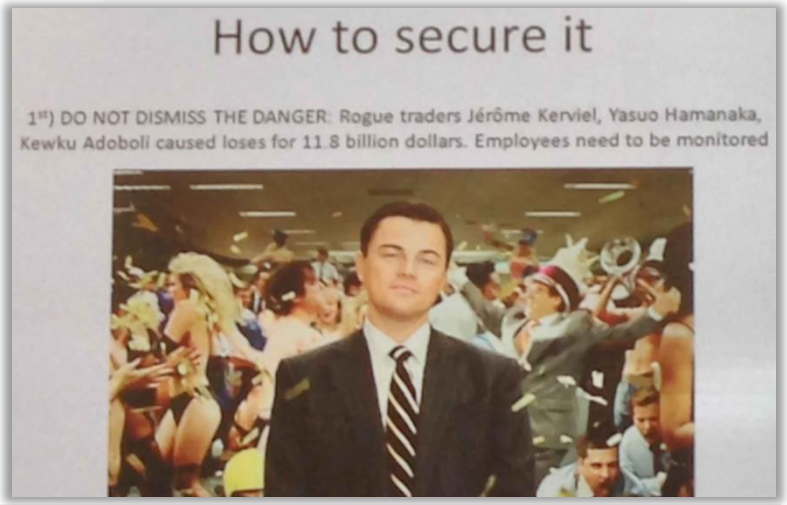
- Le **"grand casino"** fait référence aux activités des **banques d'investissement**
- **Objectifs :** exposer les vulnérabilités affectant une **solution logicielle très répandue pour les activités de trading**
- **Principe de fonctionnement de la solution :**
  - Un **client lourd Java** se connecte à un **serveur Web de fichiers**
  - Une **passerelle** qui reçoit les ordres
  - Un **base de données** qui stocke le tout

- **Vulnérabilités :**
  - **Path Traversal sur le serveur de fichiers :**
    - Permet la consultation de tous les fichiers du serveur, dont le **fichier de configuration** comprenant les **authentifiants de bases de données**
  - **Mots de passe chiffrés avec un algorithme crypto « maison »** :
    - **Clé générique** au produit qui est renseignée au sein du **client lourd**
  - **Consommation des WebServices de passage d'ordre sans authentification** :
    - Contournement des **vérifications « 4-yeux »** (front office + backoffice)
    - Les **descriptions des WebServices** étant accessibles sur le **serveur de fichiers** via la vulnérabilité Path Traversal

J3 – (In)sécurité dans le grand casino – Pablo Casais

- **Conseil de l'auteur si vous exploitez (avec succès) toutes les vulnérabilités :**
  - « Achetez un bien immobilier dans un paradis fiscal qui n'a pas d'accord d'extradition avec votre pays »

- **Recommandations pour une sécurité minimum :**
  - **Tracer les activités** des traders et le backoffice sur la solution
  - **Protéger le serveur de fichier** avec un WAF et filtrer les accès directs à la base de données
  - **Désactiver les interfaces inutiles**

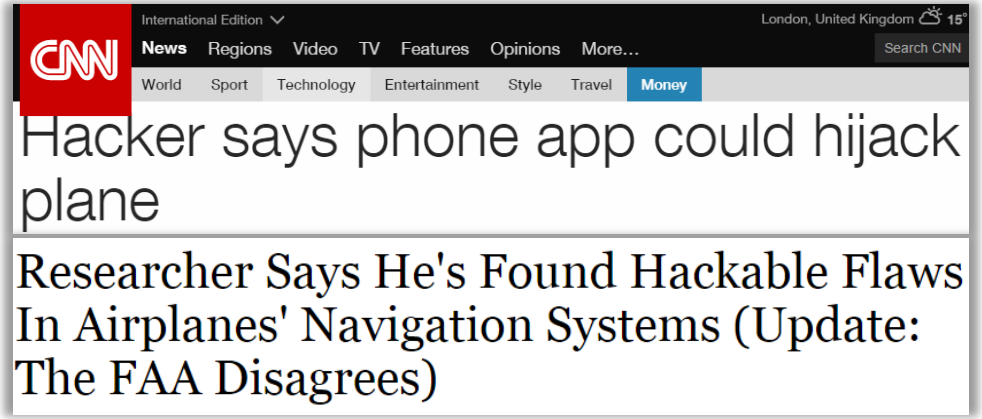


Pour résumer

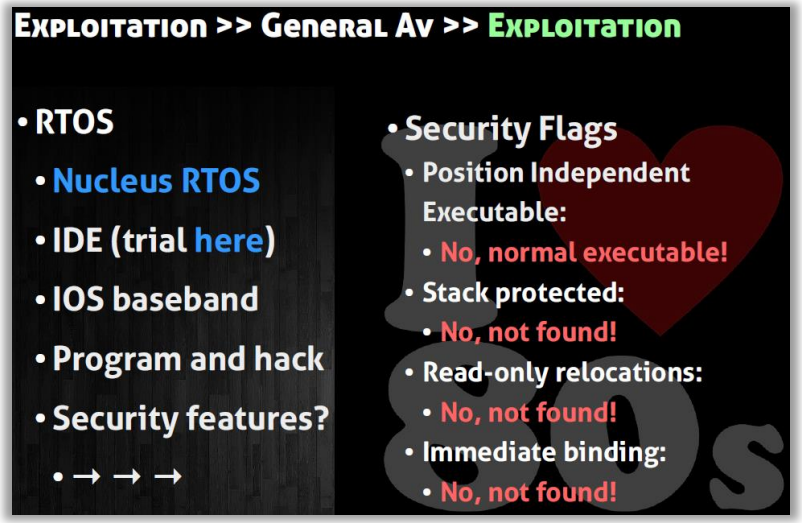
- **Des vulnérabilités triviales, dans leur découverte et leur exploitation, affectant LE produit phare du secteur**
- **Des millions à la clé**

J3 – And last but not least…– Hugo Teso

- **Hugo Teso** est le chercheur en sécurité qui avait déjà fait parler de lui **l'année dernière** en dévoilant qu'il était **possible d'attaquer un système de contrôle utilisé sur les avions commerciaux**
- **Objectifs :**
  - Présentation d'un **simulateur de gestion d'une compagnie aérienne**, qu'il a développé et qui affiche des **informations publiques** et en temps réel sur les vols dans le monde
  - Description de **l'architecture technique** des principaux produits du marché pour les systèmes de contrôle utilisés pour **l'aviation générale (loisir, tourisme, affaires) et commerciale**
  - Exposition de **vulnérabilités affectant ces produits**

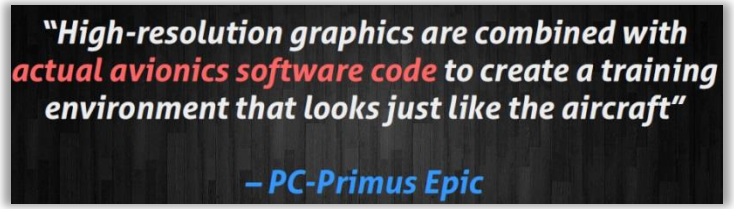


- **Vulnérabilités** pour un produit de **l'aviation générale** (Garmin Avionics) :
  - Basé sur **RTOS**
  - **Buffer-overflow dans la mise à jour des plans de vol**
  - **Aucune protection logicielle « moderne »**

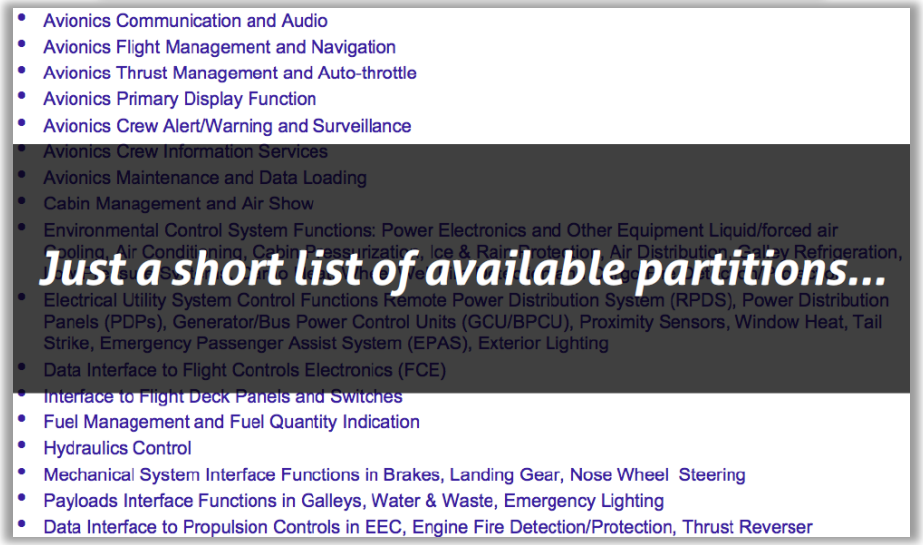


J3 – And last but not least…– Hugo Teso

- **Vulnérabilités** pour un **simulateur** de vol pour **l'aviation commerciale** (Aerosim)…
  - …mais qui est basé sur le **« véritable » code (ADA)** en fonction au sein des avions
  - **Buffer-overflow** dans une fonctionnalité de la GUI
  - Des **protections existantes contre l'exploitation mais désactivées** pour des raisons de performances



- **Exemple de post-exploitation :** s'attaquer au système *Integrated Modular Avionics* (IMA)
  - **Bus unique de données** partagé par tous les composants d'un avion. Réseau « Ethernet-like »
  - Une **API standard** standard exposée par les composants (partitions) : **ARINC 653**
  - **Pas de disjoncteur physique…**



Pour résumer

- **Des vulnérabilités classiques présentes, des protections classiques absentes**
- **Difficultés pour réaliser un PoC en condition réelle**

Résumé des autres conférences – J1

Infection BIOS, UEFI et autres : du mythe à la réalité

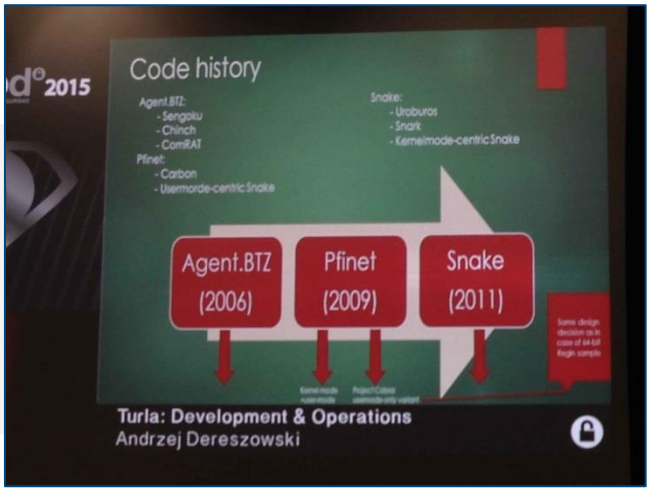
- **Rappel de l'historique des vulnérabilités et exploits visant le BIOS et plus généralement les modules physiques (SMM, PCI)**

Criminal Procedure Act: service Pack 2

- **Tenants et aboutissants quant à la mise à jour d'une loi espagnole relative à l'utilisation de traces de communication comme preuves judiciaires**
- **Évocation des problématiques inhérentes à l'utilisation de preuves numériques, notamment sur en termes "d'imputabilité des traces et données numériques à une personne physique"**

Turla:Development & Operations – the bigger picture

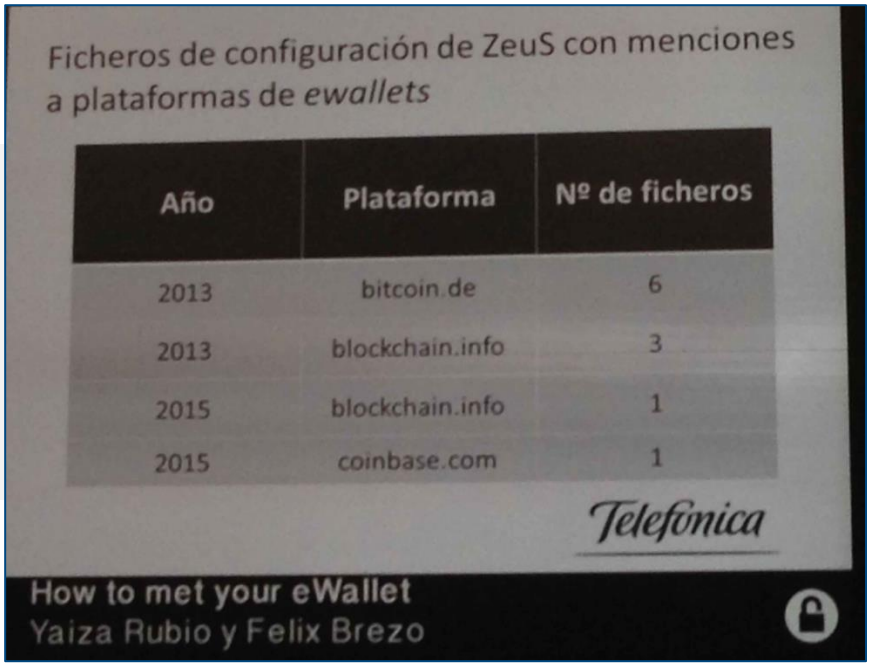
- **Détail des opérations et outils de la campagne APT "TURLA"**
- **De nombreux malwares sophistiqués développés par un même groupe qui ne serait pas lié à un état mais plutôt des cybermercenaires cybercriminels**



Résumé des autres conférences – J1

How I met your eWallet

- **Description des différents types de portefeuilles électroniques et exposer des exemples d'attaques possibles**
- **Constat sur l'intégration de plus en plus réussie de ces attaques au sein d'exploit-kits et autres malwares**



Résumé des autres conférences – J2

Finding stegomalware in an ocean of apps…

- **Pourquoi et comment analyser l'intégralité du Google Play store à la recherche de contenu stéganographié**
- **Ne rien trouver mis à part une application dédiée aux recettes de cuisine avec des drogues comme ingrédients, et une application faussement malveillante développée par une équipe de recherche d'une autre université espagnole**

Doing research about Web Application Firewalls

- **Comparer l'efficacité et le temps de réponse de 3 types de WAF :**
  - **Basé sur des indicateurs statistiques : écarts en terme de complexité entre contenu légitime et malveillant**
  - **Basé sur des chaines de Markov**
  - **Basé sur une approche de Machine Learning**
- **Le modèle statistique assure le meilleur taux de détection (99%), quasiment à égalité avec le modèle markovien mais supérieur au modèle par Machine-Learning (95%)**
- **Le modèle par Machine Learning assure une analyse rapide (0.3 ms) contre quelques millisecondes pour les autres modèles**

Résumé des autres conférences – J2

Deep inside the Java framework Apache Struts

- **Présentation de l'historique et les possibilités d'exploitation d'une vulnérabilité permettant d'éxécuter du code arbitraire sur les applications utilisant le framework Apache Struts v1 ou v2**

On Relaying NFC Payment Transactions using Android devices

- **Présentation des normes et protocoles NFC**
- **Présentation d'une attaque par relai, réalisable avec Android > 4.4, visant à faire effectuer à une victime des paiements sans contact :**
  - **La victime télécharge une application malveillante qui scan en permanence des éventuelles dispositifs NFC (CB dans la poche etc.)**
  - **L'application malveillante transmet ces informations à un terminal Android central, qui peut les rejouer sur un TPE : dans le cas d'un paiement inférieur à une certaine somme, aucune validation par un code PIN n'est requise**

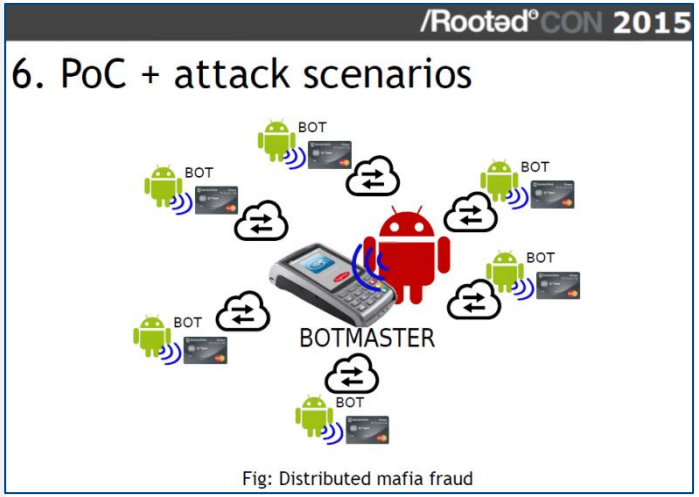


Fig: Distributed mafia fraud

Résumé des autres conférences – J2

Rouges et Bleues : deux équipes, deux saveurs

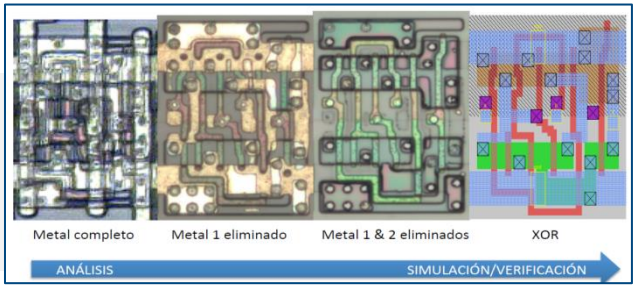
- **Présentation d'un top 5 des TTP (Tools, Techniques and Procedures) les plus utilisés, rapides et efficaces mis en œuvre par les Red Team et à mettre en œuvre par les Blue Team sur différents thèmes (gestion des authentifiants, vulnérabilités applicatives, attaques réseau, escalade de privilèges, infiltration et exfiltration)**

Le temps entre mes mains

- **Présentation des méthodes pour désactiver HSTS : utiliser NTP pour changer l'heure du système, dans la mesure où la plupart des navigateurs l'utilisent comme référence temporelle**
- **Exemple d'impact suite à la modification de l'heure du système : déni de service sur les tâches planifiées Windows**
  - **La date de l'exécution N+1 d'une tâche est calculée lors de l'exécution N : si l'exécution N n'a jamais lieu, les futures n'auront également pas lieu**
  - **Intéressant dans le cas de tâches de mises à jour systèmes (par ex. via WSUS)**

Ingénierie inverse de circuits intégrés

- **Comment décapsuler, analyser, modéliser un cryptoprocesseur d'une borne d'arcade des années 80 pour casser la protection anti-copie**



Résumé des autres conférences – J3

Bend the developers to your will

- **"Développeurs, ne compilez pas du code récupéré auprès d'une source non fiable (github, internet etc.)...il est très simple pour un attaquant d'y cacher du code malveillant."**
- **Exemples pour Make, MsBuild, Gradle, Xamarin et Visual studio**

Amplification de l'arsenal d'outils pour les attaques WiFi

- **Une suite de scripts Python pour réaliser des attaques WiFi, et qui ne sont pas basés sur la célèbre suite Aircrack**
- **Comment fabriquer une structure en bois qu'il est possible de cacher dans un coffre de moto, et y positionner une station d'interception WiFi avec des antennes omnidirectionnelles auto-rotatives orientées par des petits moteurs**

Physical Penetration Testing

- **Tous les trucs et astuces pour mener à bien une intrusion physique**
- **Comment contourner les controles d'accès par badge, détecteurs de mouvements (chaleur/IR, photosensibles), alarmes et serrures magnétiques**

Résumé des autres conférences – J3

Can I play with madness ?

- **Présentation de l'outil propriétaire "Path5" développé par une équipe de la société ElevenPath et qui consiste en une gigantesque base de données récupérant automatiquement toutes les applications gratuites disponibles sur Google Play**
- **Comment une analyste peut utiliser cette plateforme pour corréler des informations, et par exemple rechercher des faux comptes développeurs et producteurs de malwares**

Android: Back to the Future (Too? or Two?)

- **Android effectue les recherches de mise à jour en HTTP via le protocole de sérialisation "protobuf" made in Google**
- **Il est ainsi possible d'altérer ses requêtes et "mentir" sur la version courante du terminal pour le downgrader**

Bypassing DRM Protections at Content Delivery Networks

- **Présentation de l'architecture typique des diffuseurs de contenu vidéo en ligne pour Nubeox, Netflix, WuakiTV, TotalChannel, Orange TV**
- **La plupart des acteurs utilisent des clients lourds et imposent des limitations qu'il est possible de contourner (identification par IP, hash généré côté client etc.)**

En conclusion

- Un nombre élevé de conférences :
  - 24 talks en 3 jours, un record absolu
- Différents types d'interlocuteurs :
  - Hackers stars, professionnels de la SSI, chercheurs académiques, amateurs, avocats etc.
- Des conférences de très bonne qualité dans l'ensemble :
  - Sur des sujets pragmatiques
- Un cadre fort agréable tout en restant financièrement abordable

The power of simplicity
«Ce qui est simple est fort»

www.solucom.fr

Contact

Thomas DEBIZE
Consultant

thomas.debize@solucom.fr