Morceaux choisis

OSSIR 10 septembre 2013

Boris HAJDUK

viaded

BlackHat USA 2013

- 2 jours au Caesar Palace 31/7 – 1/8
- 101 conférences (9 tracks)
- 48 security tools présentés au salon Arsenal
- 8 workshops de 3h ou 4h
- 12 sponsored workshops d'outils commerciaux
- 1800 USD
- Jamais de manque de place

Keynote du directeur NSA

link

Section 215 Authority: metadata téléphoniques

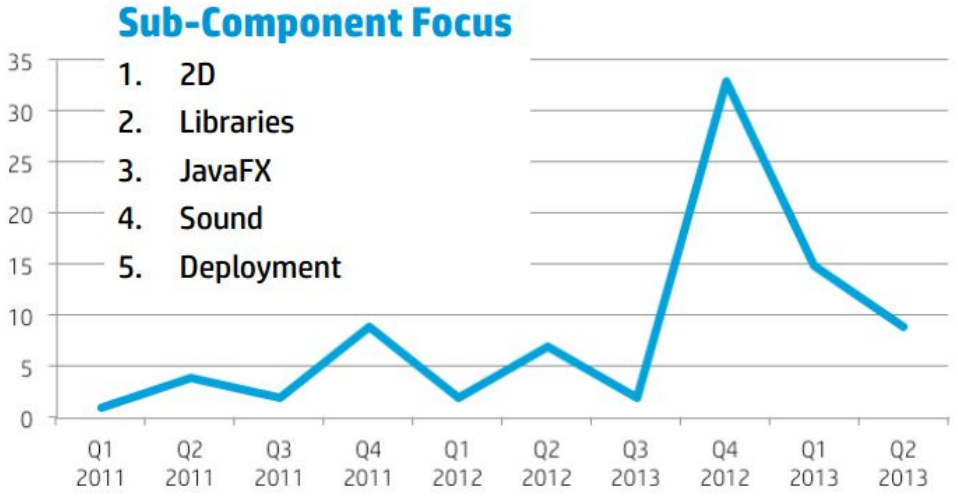
Section 702 Authority: interception réseau (abroad, no US person) --> Industry is compelled to comply.

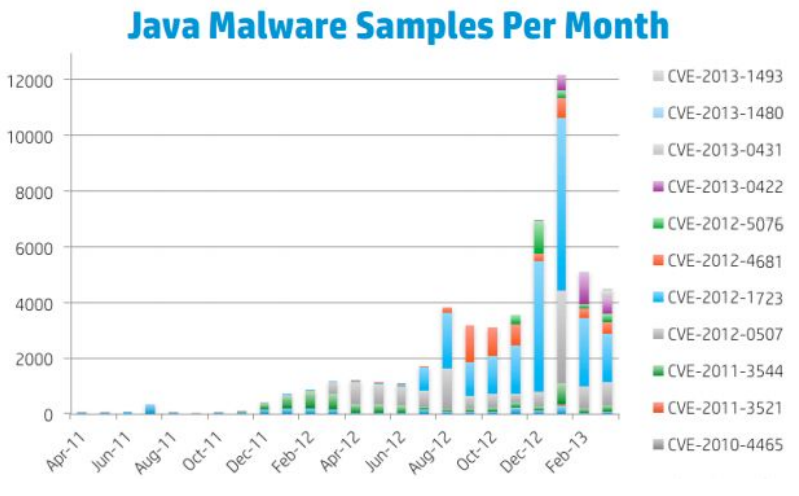
Justification: ça a évité 54 activités terroristes

Audit internes/externes: pas d'exceptions relevées. They could, but they don't.

Java every-days (ZDI) link

- 93% of Java users not running latest patch 1 month after release
- Analyse statistique ZDI 2011-2013:
  - patchs: composants les plus souvent patchés
  - submissions ZDI: les modules les plus attaqués
  - malwares in the wild: corelated w/ submissions





Build a SpyPhone on Android link

- Modification d'application pour ajouter un spyware
  - apktool decode angrybirds.apk
  - copier/coller un répertoire et modifier le manifest --> ajout d'un service
  - apktool rebuild AngryBurds birdsbad.apk

- Self-sign l'APK car n'importe quel certificat est OK, pas besoin d'être signé par un CA.

  (angrybirds a des certificats cassés: valid-from et valid-to inversés, mais marche quand même

  --> Android vérifie mal les signatures et certificats

- Pas d'interface utilisateur pour voir qui a signé une application

Power Analysis for cheapstakes

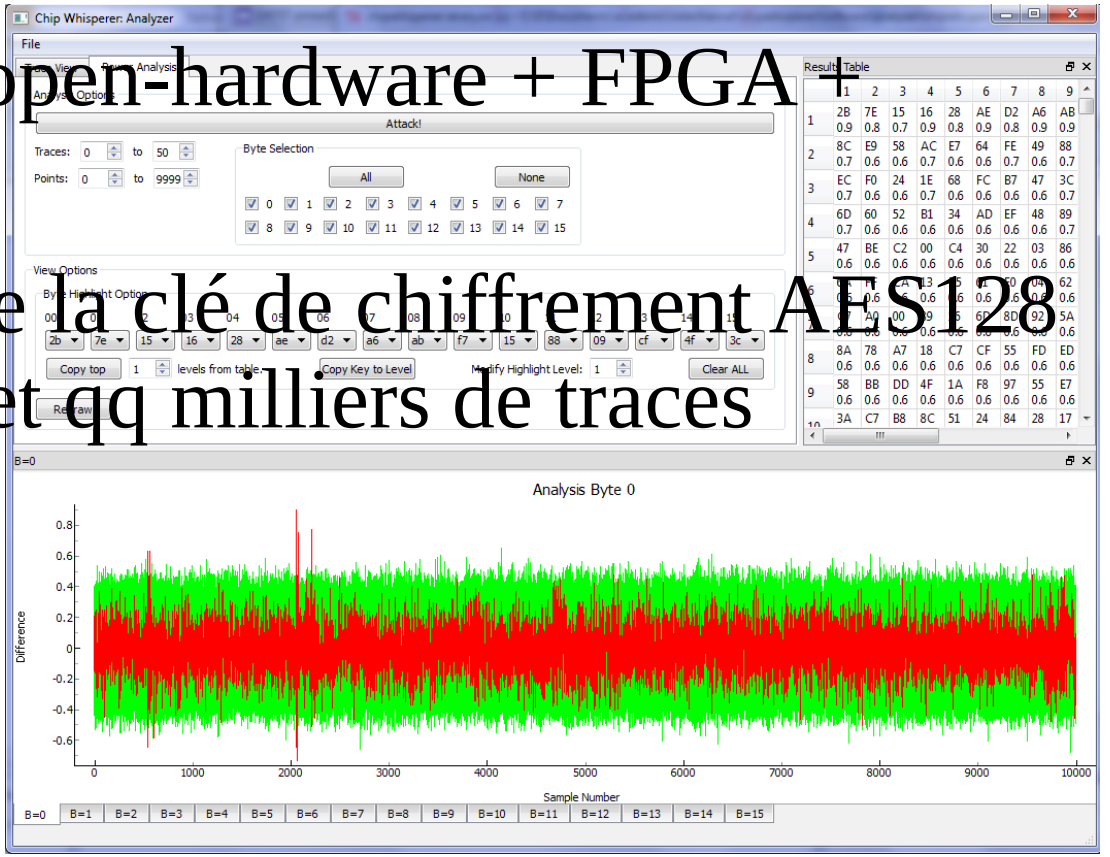
link

- Analyse de la consommation de courant d'un chip de chiffrement

  --> forcer des déchiffrements sur du contenu invalide

- chipwhisperer.com : open-hardware + FPGA + open-software
- Démo live : détermine la clé de chiffrement AES128 en quelques minutes et qq milliers de traces

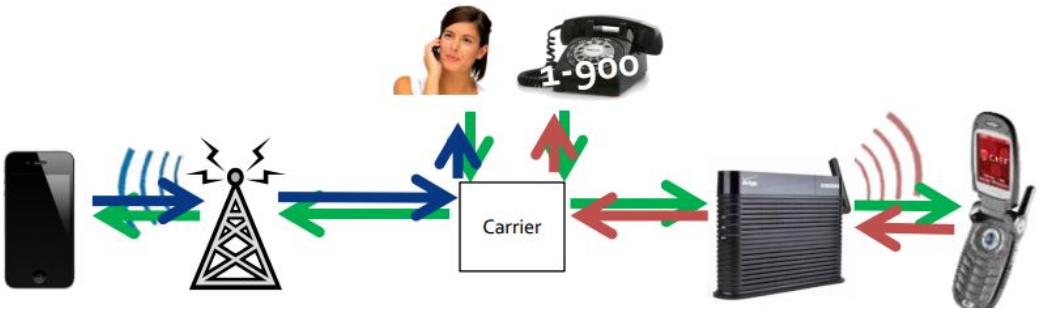
  --> 1100$ full set



Phone interception & remote cloning with CDMA femtocell Verizon

link

- Basé sur l'attaque femtocell SFR de 2011
- Root login sur port série intégré
- Bcp de dev : module kernel pour interception IPsec, Wireshark dissector pour protocole EVRC
- Démo live interception appel, sniff SMS, sniff Data (!) et cloning.
- Conseil de fin: Wifi calling with IPsec/SSL.... mais c'était avant les nouvelles révélations de Snowden



XSS Defense on the Battle-Front

link

Idée générale : ModSecurity à toutes les sauces

1. détection XSS à la demande avec OWASP ZAP -> XML report -> ModSecurity rule
2. détection XSS à la volée ModSecurity + arachni + phantomJS (+ beef)
3. ModSecurity pour générer des CSP policy à la volée
4. Ajout de sandbox JS à la volée avec MentalJS

Pass-the-Hash 2 link

- GPP Group Policy Prefs: easy way to enforce settings on every workstation

  --> Popular with administrators to set passwords
- Passwords chiffrés avec AES-256... avec une clé publiée dans MSDN http://msdn.microsoft.com/en-us/library/cc422924.aspx
- Bonus: pass the hash avec des smartcards
- Liste de préconisations (en supplément à celles de M$) pour se protéger contre PtH

All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.<2>

The 32-byte AES key is as follows:

```
4e 99 06 e8  fc b6 6c c9  fa f4 93 10  62 0f fe e8
f4 96 e8 06  cc 05 79 90  20 9b 09 a4  33 b6 6c 1b
```

```
PS C:\demo> Get-DecryptedCpassword "9KQYhHxSxrrZjFo8Frt/nExdMLKsQM+ThhWOJKajaRc"
Recycling*3ftw!
PS C:\demo>
```

SQL Injection optimization & obsfucation techniques

link

OPTIMIZATION

- Accélérer les blind-injections : nb de requêtes/char -30%
- binsearch-tree, regex, bitwise, bin2pos : binary_most_common_letters_first
- Encore mieux: trigraphes les plus fréquents : THE, AND, THA, ENT...

OBSFUCATION

- Allowed whitespaces for different DB engines
- Bypass ModSecurity, Fortinet, GreenSQL
- réf: http://websec.ca/kb/sql_injection

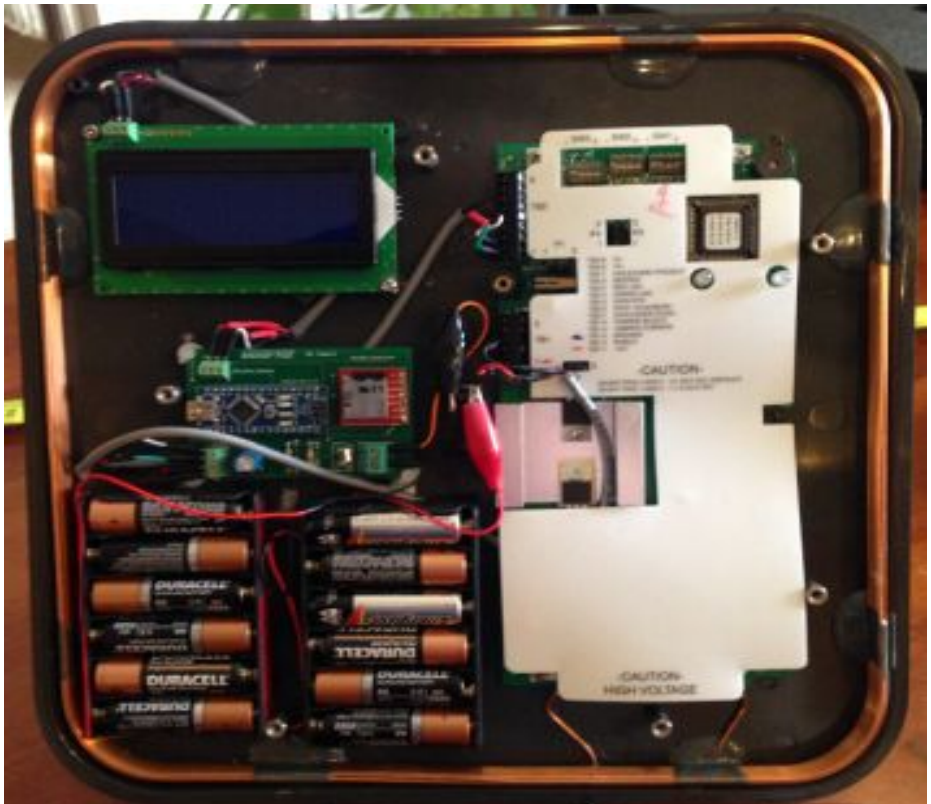
RFID Hacking link

Constat: la principale difficulté pratique: la lecture des cartes avec proxmark

-> lecteur de parking "long range" 30x30cm dans un cartable (200-400$)+ arduino

-> lecture à 90cm

- ...puis card cloning

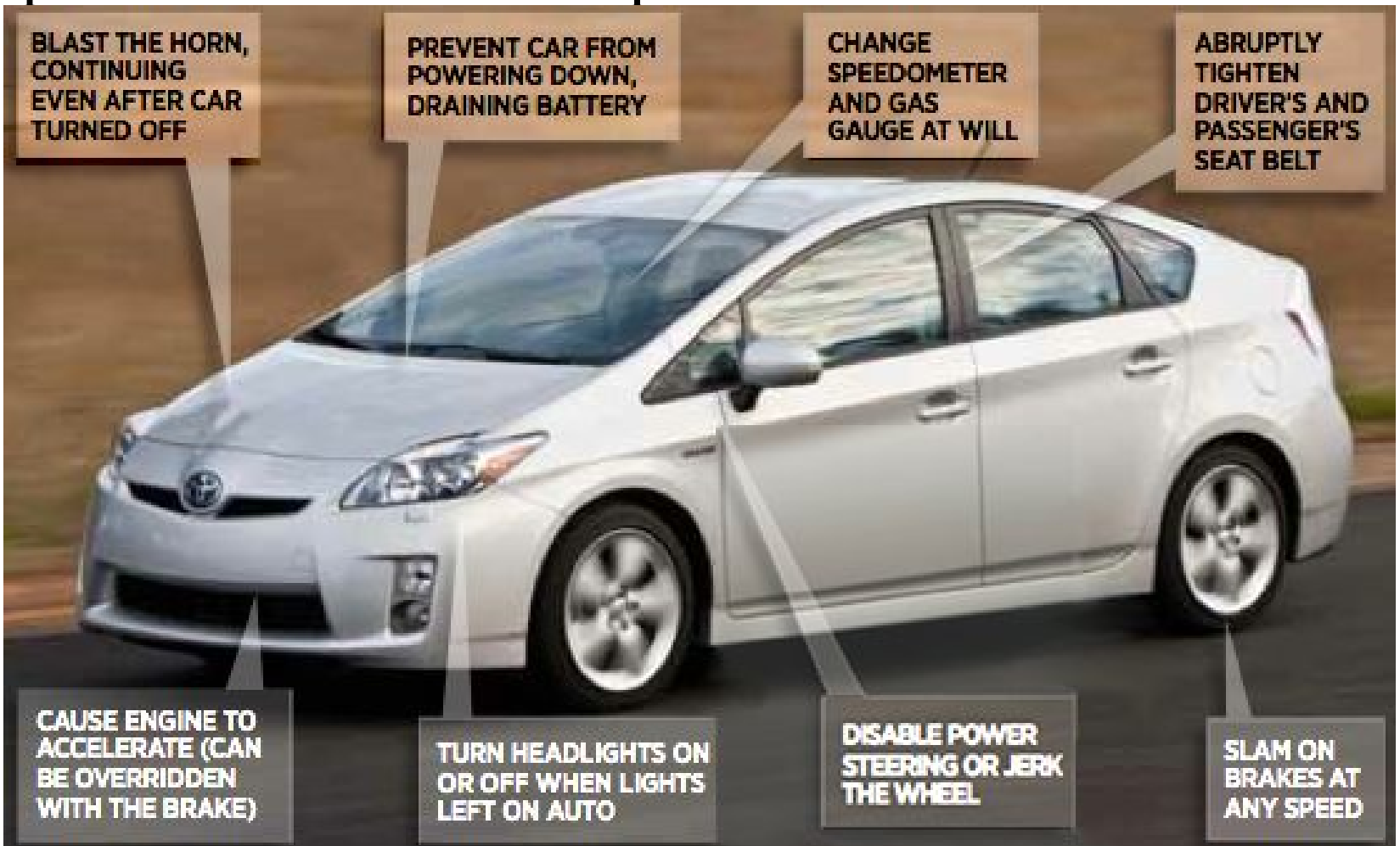


Defcon 21

- 3,5 jours au Rio 2/8 - 4/8
- 114 conférences (5 tracks)
- workshops social engineering, lockpicking, tamper evidence, CTF, password crack, hardware hacking
- 180 USD (10x moins cher que blackhat)
- un public plutôt citoyen que pro; les salles sont souvent trop petites

Prius 0wned (Miller+Valasek) link

- Seul critère d'achat: “Can it park itself ?”
- Spoof CANbus + attaque du “firmware” des ECU

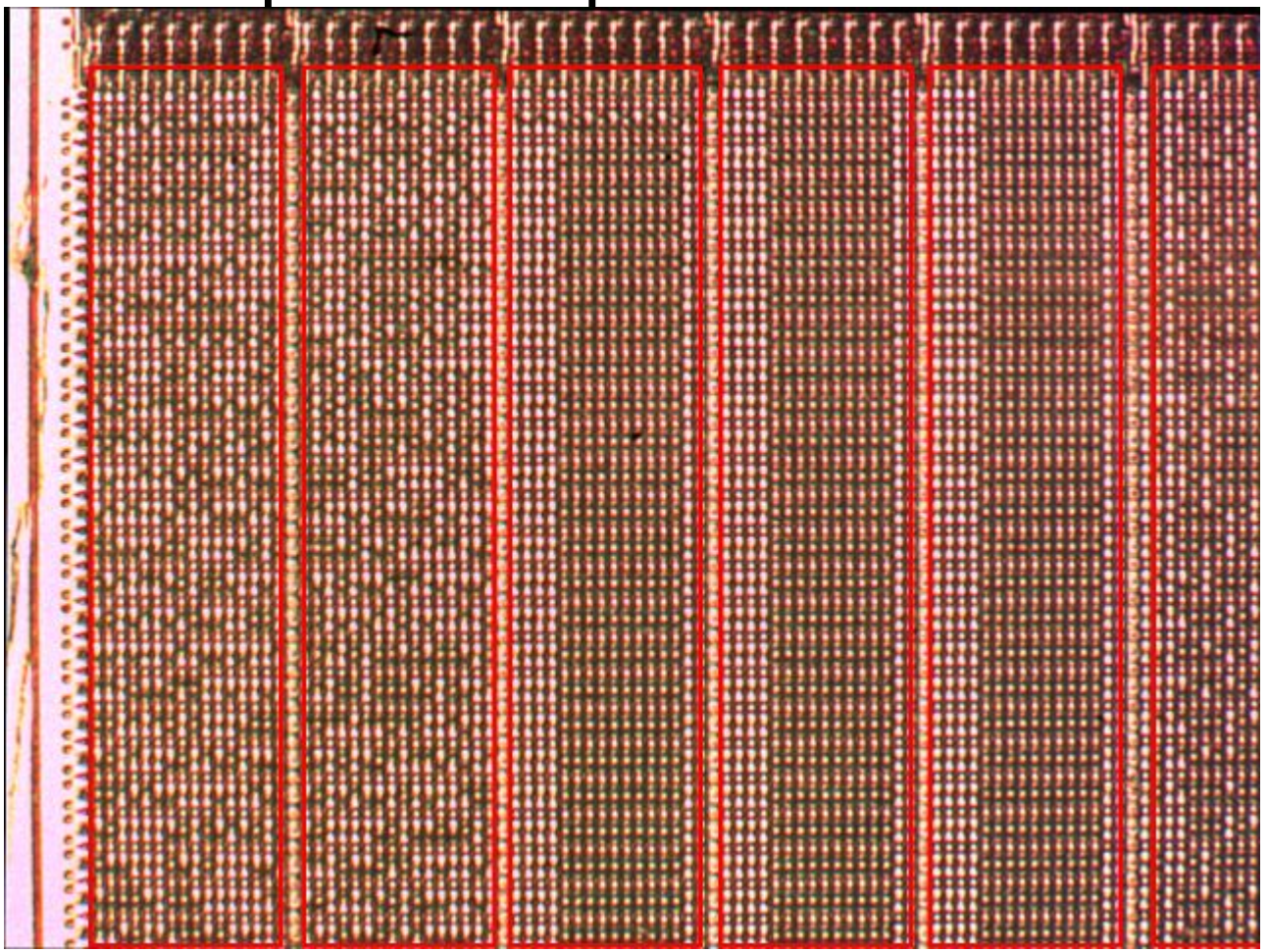


Decapping chips the easy/hard way

link decapping

link OCR

- Techniques chimiques/physiques
- OCR pour dumper le contenu d'une ROM !



Hack billet NFC de tramway italien link

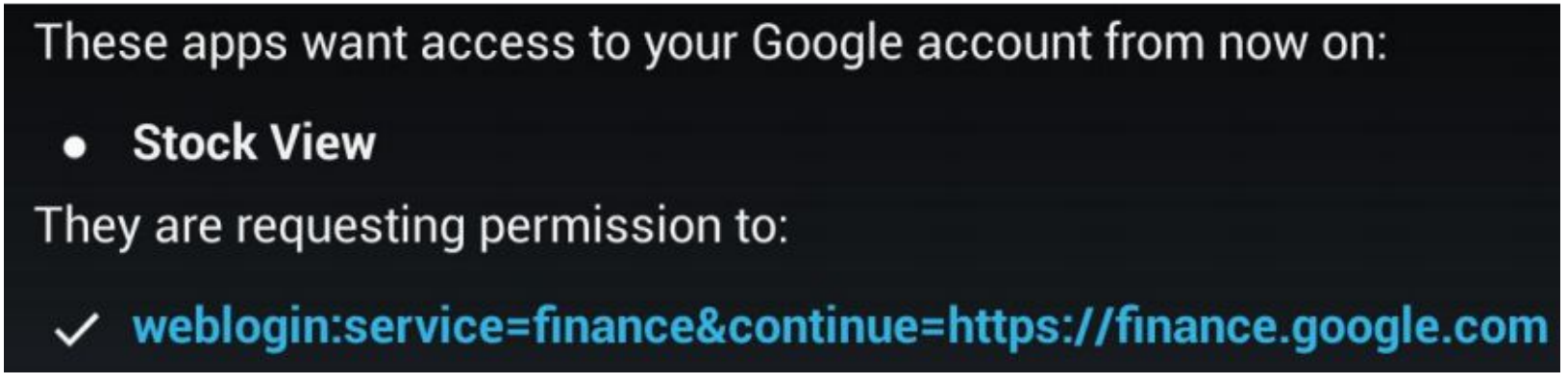
- NXP Mifare Ultralight : 2012: SF, Boston, DC, Seattle, NJ, Salt Lake City, Chicago, Philadelphia... 2013: Turin, now with OTP.
- Lock OTP (one-time programmable bits) pour ne pas pouvoir effacer de tickets
- Timestamp en écriture

  --> Android app NFC

Android weblogin: Google skeleton key

link

- Weblogin can bypass password prompts
- 1 token can fully compromise Google Apps
- Cookies obtained are not limited by service
- App may ask for YouTube and then read your email
- Bonus if the user is a Google Apps Admin !
- Live Demo Google Finance



Hacked @ Las Vegas

- Cell phones
- Cisco IP phones
- Printers
- Cisco routers
- Cisco switches
- Toyota Prius
- Ford Escape
- Mini Cooper
- Home cable-routers
- Iphone docking station
- Toilettes BlueTooth !
- Robot lapin Karrotz
- Webcams wifi
- Prise électrique connectée
- Sonos Bridge
- 2 boitiers domotiques
- Ticket de traway
- Physical locks
- Electronic locks
- Femtocells

Documents

- Defcon 21 PDF: http://contagiodump.blogspot.com/2013/08/defcon-21-archives-speaker-materials.html
- BlackHat USA 2013 PDF: https://www.blackhat.com/us-13/archives.html
- Bonus: vidéos des B-Sides: https://archive.org/details/bsideslv2013