TEHTRI-Security

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

Web In The Middle – Attacking Clients

www.tehtri-security.com

Speaker

- Laurent OUDOT
  - Founder & CEO of TEHTRI-Security (2010)
    - http://news.google.com/news/search?q=tehtri-security
  - Senior Security Expert
    - When ? 15 years of IT Security
    - What ? Hardening, pentests...
    - Where ? Hired for highly sensitive networks & systems

      e.g: French Nuclear Warhead Program, United Nations, French Ministry of Defense…
  - Research on defensive & offensive technologies
    - *Past: Member of the team RstAck & of the Steering Committee of the Honeynet Research Alliance...*
    - Frequent presenter and instructor at computer security and academic conferences like Cansecwest, Pacsec, BlackHat USA-Asia-Europe, HITB Dubai-Amsterdam, SyScan Singapore-China, US DoD/US DoE, Defcon, Hope, Honeynet, PH-Neutral, Hack.LU
    - Contributor to several research papers for SecurityFocus, MISC Magazine, IEEE, etc.

Introduction

- Goal:

  Let's talk about security issues related to attacks against Web clients in an insure environment where Man in The Middle actions might occur.

- Target audience:
  - White hats, to fight Cybercrime, Business Intelligence, Information Warfare…
- Notices:
  - 1 hour talk: with as many concepts & demo as possible, but this could take days to show everything.
  - Legal Issues: we remind you to carefully apply the laws in your countries before applying techniques like ours.
  - Legal Issues: we cannot show everything ☺

Plan (Web In The Middle)

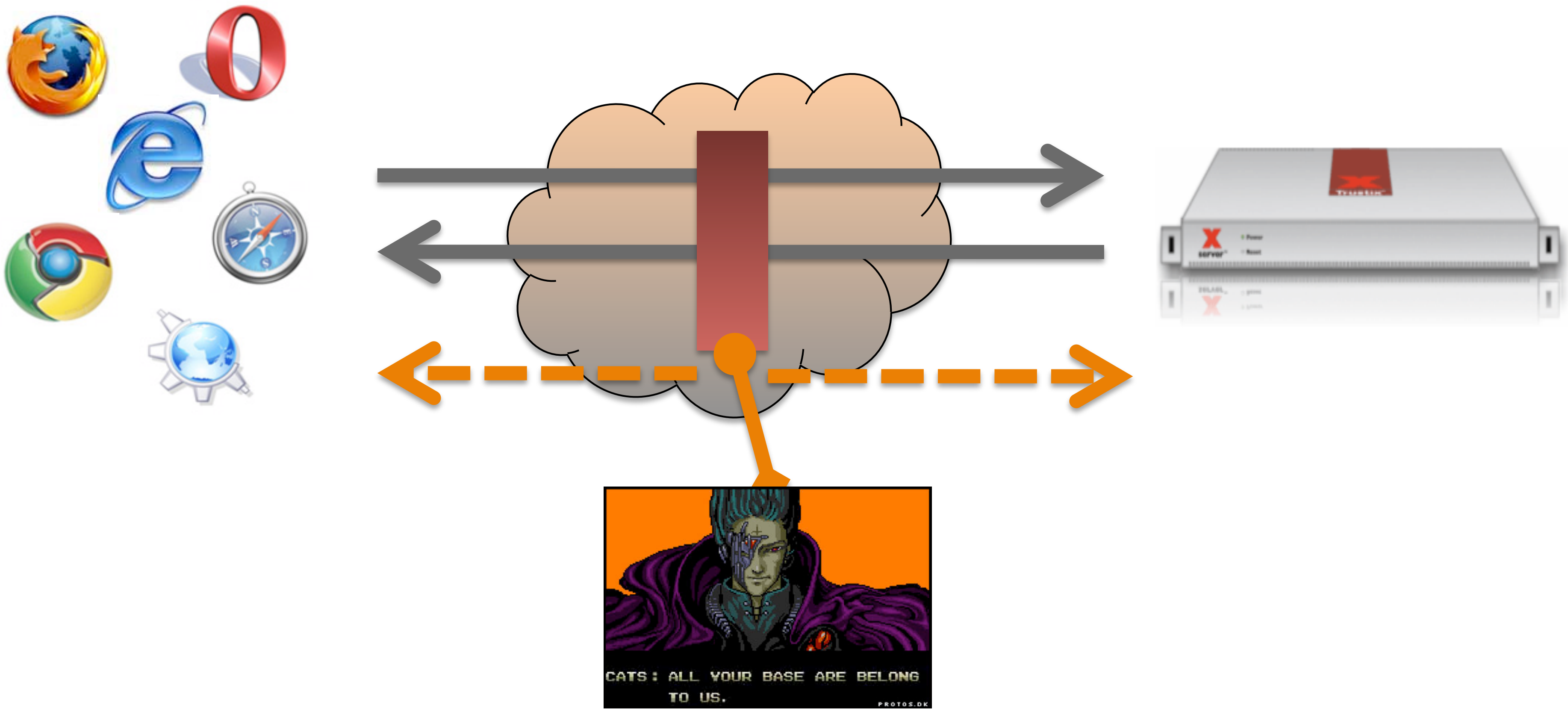
- Theory
- Some examples
  - Web services
  - Web applications
  - Handled devices
- Conclusion

I) THEORY

Web In The Middle

- Man in the Middle attacks are well known and documented for years
  - The concept is that an external entity is able to participate to network discussions between some peers
- We will focus at some security issues related to those threats, in the Web environment

Web In The Middle



Impacts

- Low-level layers might be controlled by a malicious attacker
- We cannot trust those layers
- Potential classes of issues
  - Confidentiality
    - Example: Data stolen (Passwords…)
  - Integrity
    - Example: Data modified (Injection of evil payloads…)
  - Availability
  - Authenticity
  - Non-repudiation

Workaround

- Security added at the upper layers
  - Authentication
  - Ciphering
  - …
- Solutions
  - VPN
  - SSL
  - …

Potential remaining issues

- The final level of security will be based on the upper layers adding security
- We need to be sure of those layers
  - VPN Issues
  - SSL Issues
    - sslstrip (!) http://www.thoughtcrime.org
      - U+FF0F → ／ (/)

HTTPS & HTTP

- http://ocsp.verisign.com/

```
POST / HTTP/1.1
Host: ocsp.verisign.com
User-Agent: Mozilla/5.0 (X11; U; Linux i686; ru; rv:1.9.1.1)
   Firefox/3.6.3
Accept: text/html,application/xhtml+xml,application/
   xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Content-Length: 115
Content-Type: application/ocsp-request
0q0o0M0K0I0 +
```

WITM ?

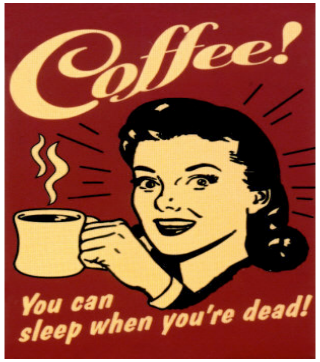
- We know that solutions exist to avoid WITM (SSL…)
- So, now let's consider that we are luckily browsing the web without those problems :
  - What might happen then ?
- Where exactly can we be targeted through Web In The Middle Attacks ?
  - Wired World
    - Many LAN are still vulnerable to layer 2 attacks so that an attacker can redirect your traffic to his evil computer
    - Where redirections attacks work (ARP Spoof…)
  - Wireless World
    - Public & Private HotSpots with signal that can be intercepted
      - Wifi signal (some companies prefer to harden those sessions through the use of EDGE/3G networks, etc)

Many targets

● ● ●

Targets everywhere

Home

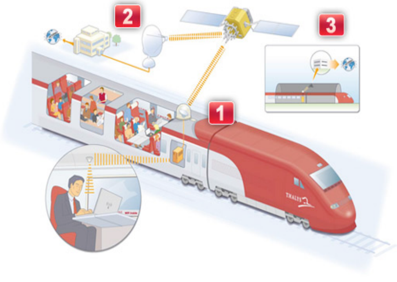


Coffee/Bars

Restaurants

Hotels

Corporate…



Trains

Planes

Bus

Taxis / Cars

● ● ●

Wild Wild Web

- You gonna claim that:
  - – Everything is done properly for your security (SSL, etc),
  - – Connecting yourself to such a network, or such web sites, sounds safe, etc.
  - – You already know those threats, etc.
- Don’t you ?

Wagon attacked (old school)

courtesy of www.charlesmarionrussell.org

Nowadays…

Hackers

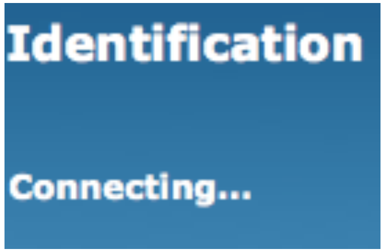
TARGETS
In
WAGON

Cyber-Attack in a Train

Comfort 1
Internet available

- Example: Thalys
  - Notice: Comfort is full of Businessmen…
- Register your account on the Thalys
  - It’s just 1 HTTP request
  - URL
    - http://portal.thalysnet.com/index.php?doAction=register
  - VULN: Clear text HTTP Traffic

```
POST /index.php?doAction=register HTTP/1.1
Host: portal.thalysnet.com
Email=…&name=…
&firstname=…&zip=…&country=…
&pass1=
&pass2=
&secretquestion=q1
&secretanswer=
&doAction=register1stepfinal&showAction=register1step&acceptgc=yes&autologin=yes
```



Identification

Connecting…

Examples of vulnerabilities

- Bonus:
  - VULN: Each time you login, l/p will be sent through HTTP clear text channel (& cookies contain password)
  - VULN: Each time you consult a ThalysNet service, you send the cookie (with your password)
    - Example: consult the map (where are you on earth?)
- We found many vulnerabilities without doing any attack, just by using the service with no offensive method
  - THALYSNET has been contacted with some vulns
- We cannot display everything here
  - Legal issues
  - We just hope that this might help at improving this service and that end users will take care in the future

Problems

- Many remote Internet Services (on the web) do not use (100%) secure channels between you & them
  - When SSL is available there, it might not always be applied at anytime
- Many local applications (on your devices) do not use (100%) secure channels anyway
- Most clients announce their real version of User-Agent
  - Which really helps to choose an exploit…

Dangerous behaviors of web sites

- Security Problems on the web sites
  - Login Phase
  - Session
  - External data retrieved
  - Logout Phase
  - …
- When you are lucky, they just provide SSL for the login phase, and then the war begins…

Dangerous behaviors of applications

- Security problems on the clients (applications)
  - Installation (remote licenses, resources…)
  - Initialization (for each running)
  - Dynamic configuration (grabbed remotely)
  - Dynamic data retrieved remotely (e.g: rss…)
  - Dynamic data put remotely (e.g: statistics…)
  - Remote Login
  - Remote session
  - Remote Logout
  - Remote updates
  - …

2) SOME EXAMPLES

2.1) APPLICATIONS

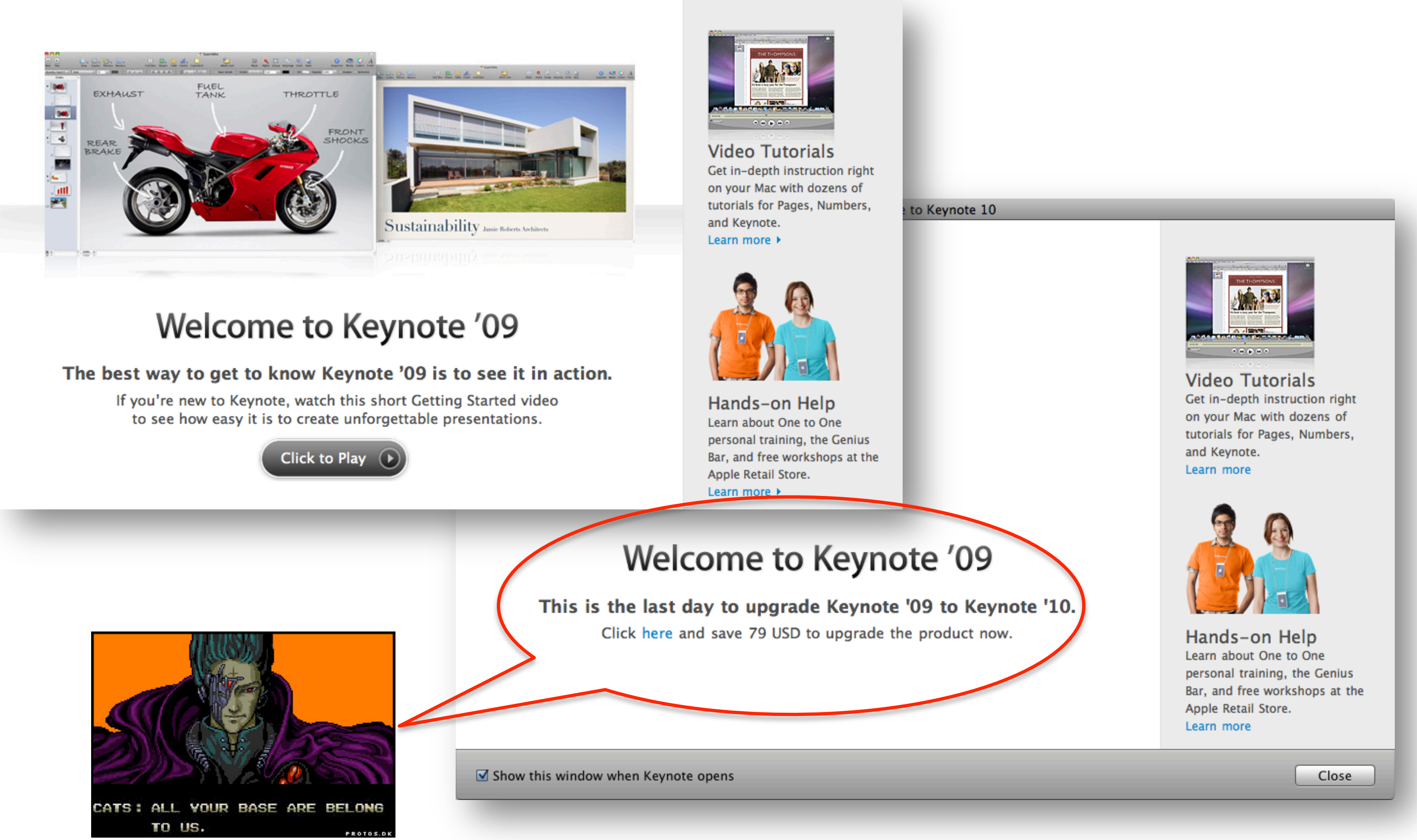
Initialization issues

- Mozilla products
  - You think that you just opened your laptop to read your emails through TLS/SSL session with your remote mail server ?
  - No, there might be outbound HTTP traffic with clear text channel (default config)
    - http://live.mozillamessaging.com/%APP%/whatsnew?locale=%LOCALE%&version=%VERSION%&os=%OS%&buildid=%APPBUILDID%
  - Thunderbird, default web page during launch
    - E.g: http://live.mozillamessaging.com/thunderbird/start?locale=en&version=3.0.4&os=Darwin&buildid=20100317134139

Initialization issues

- Apple products
  - You think that you just opened your laptop to work on local documents with iWork09 or iLife09 ?
  - No, there might be outbound HTTP clear text traffic (popup of initialization)
    - http://www.apple.com/welcomescreen/ilife09/iphoto/
    - http://www.apple.com/welcomescreen/iwork09/numbers/
    - http://www.apple.com/welcomescreen/iwork09/keynote/
    - http://www.apple.com/welcomescreen/iwork09/pages/
      - "GET /welcomescreen/iwork09/pages HTTP/1.1 »
      - "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_3; en-us) AppleWebKit/533.16 (KHTML, like Gecko)"

Client-Side Attacks + Fishing + …



Welcome to Keynote '09

The best way to get to know Keynote '09 is to see it in action.

If you're new to Keynote, watch this short Getting Started video to see how easy it is to create unforgettable presentations.

Video Tutorials

Get in-depth instruction right on your Mac with dozens of tutorials for Pages, Numbers, and Keynote.

Hands-on Help

Learn about One to One personal training, the Genius Bar, and free workshops at the Apple Retail Store.

Welcome to Keynote '09

This is the last day to upgrade Keynote '09 to Keynote '10.

Click here and save 79 USD to upgrade the product now.

Video Tutorials

Get in-depth instruction right on your Mac with dozens of tutorials for Pages, Numbers, and Keynote.

Hands-on Help

Learn about One to One personal training, the Genius Bar, and free workshops at the Apple Retail Store.

☑ Show this window when Keynote opens

Initialization issues

- Microsoft products
  - You think that you just opened your laptop to work on local documents with Office 2007 ?
  - No, there might be outbound HTTP clear text traffic

```
POST /Services/subscription.asmx HTTP/1.1
Content-Type: text/xml; charset:utf-8
Accept: auth/sicily, */*
SOAPAction: "http://schemas.microsoft.com/officelive/soap/
   GetWebAccountInfo"
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1;
   WOW64; Trident/4.0; GTB6.4; SLCC2; .NET CLR 2.0.50727; .NET
   CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
   OfficeLiveConnector.1.4; OfficeLivePatch.1.3)
Host: workspace.office.live.com
```

- ...

Updates issues

- Tool « ISR-evilgrade »
  - Infobyte Security Research
  - www.infobyte.com.ar
  - Automatic attacks against many products while they try to update
    - Java plugin, Winzip, Winamp
    - MacOS, OpenOffice, iTunes
    - Linkedin Toolbar, DAP [Download Accelerator]
    - notepad++, Speedbit
- TEHTRI-Security found known « Security Products » that update through clear text HTTP channels…
- It’s pretty dangerous to trust the update actions while you are in an evil environment (but would you like to keep an outdated version of a product ? Dilemma…)
- You should also look at the amazing tool “Karmetasploit” if you want to have more fun than just looking at updates issues…

2.2) WEB SITES

What about web sites ?

- Initial page
  - What: Where it generally contains the source code (HTML FORM) to login.
  - Risk: No HTTPS here implies that the action of the Form might be changed to HTTP (no HTTPS!) or to something else that would be evil
- Login/Password
  - What: This is the transaction carrying the login & password of the end user
  - Risk: No HTTPS here implies that loss of confidentiality
- Complete Session
  - What: This is the session between browser & web site
  - Risk: No HTTPS means loss of confidentiality, and you might not be able to logout (fake logout hyperlink)…
- Logout link
  - What: the hyperlink/form used to logout
  - Risk: No HTTPS → You cannot be sure that you are logued out, maybe you received a fake logout HTML result, etc
- SSL ready
  - What: The default behavior is to use HTTP but we could use HTTPS by rewriting the links, etc, so that the web site become HTTPS only (or almost only)
  - Risk: A non SSL ready web site means that you cannot have full SSL sessions

What about famous web sites ?

June 2010	Initial Page	Login/ Password	Complete Session	Logout Link	SSL Ready ?
Hotmail	HTTP	HTTPS	HTTP	HTTP	NO
Yahoo	HTTPS	HTTPS	HTTP	HTTP	NO
LinkedIn	HTTP	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 ☺

Google++

*« Over the last few months, we've been researching the security/latency tradeoff and decided that **turning https on for everyone was the right thing to do** »*

- Sam Schillace, **Gmail** Engineering Director, January 12, 2010

« Google understands the potential risks of browsing the web on an unsecured network, particularly when information is sent over the wire unencrypted — as it is for most major websites today.

*(…) As we work to provide more support for SSL across our products, today we're introducing the ability to **search with Google over SSL**. »*

- May 21, 2010 Murali Viswanathan, Product Manager

« HTTPS Everywhere »

- Firefox extension (collaboration between The Tor Project & the Electronic Frontier Foundation)
  - https://www.eff.org/https-everywhere
- Many sites on the web have limited support for encryption over HTTPS (difficult to use).
  - Example: default to unencrypted HTTP, or fill encrypted pages with links that forces unencrypted traffic.
- HTTPS Everywhere extension rewrites all requests to compatible sites with HTTPS
  - Google Search, Wikipedia
  - Twitter, Facebook
  - The New York Times, The Washington Post
  - Paypal, EFF, Tor, Ixquick…

ELECTRONIC FRONTIER FOUNDATION

Reminder

- MITM against Web clients
  - Confidentiality: credentials, data…
  - Integrity: XSS/CSRF, Client-side attacks…
  - …
- Pretty easy to handle
  - DNS, ARP, etc + 302 or Code Injection or …
- Bonus
  - Most applications on embedded devices do not use HTTPS for the session

2.3) LAN ATTACK (REMOTE)

Remote LAN Attack

- Upgrade your power on a remote LAN
  - Phase 1, own the traffic
    - Internal DNS access
    - ARP spoofing
    - DNS Cache Poisoning
    - DHCP spoofing
  - Phase 2, inject evil traffic
- Very usefull to bounce in a LAN or from a LAN to another…

2.4) HANDLED DEVICES

Looking at web applications

- Let’s look at applications that are installed on devices like phones, etc
- Most of them don’t really use HTTPS
- They use HTTP
- Many individuals and companies use it on hotspots (airport, coffee…)
- The only complex things to handle for a MITM attacker might be the encoding issues (gzip/deflate) & some specific formats of data

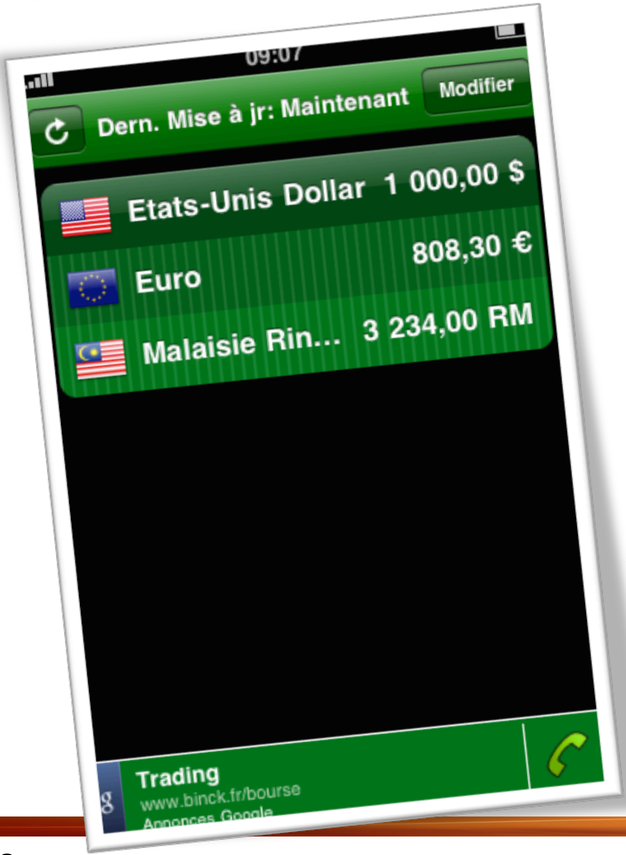
Example

- Here is a random application that need to download information to work
- It’s a currency converter (sure we need the latest data ☺)
- It connects to a remote web server
  - – http://iphonecurrencyconverter.appspot.com/
  - – "GET /json HTTP/1.1"
    - "Currency/2.1 CFNetwork/459 Darwin/10.0.0d3"
- The data are easy to analyze

{"USD": 1.0000, "SYP": 45.4500, "LAK": 8476.00, "RSD": 67.2072, "KHR": 4115.00, "GYD": 205…

Inject fake data

- Very easy to inject fake data…
- What would happen on more sensitive applications…?

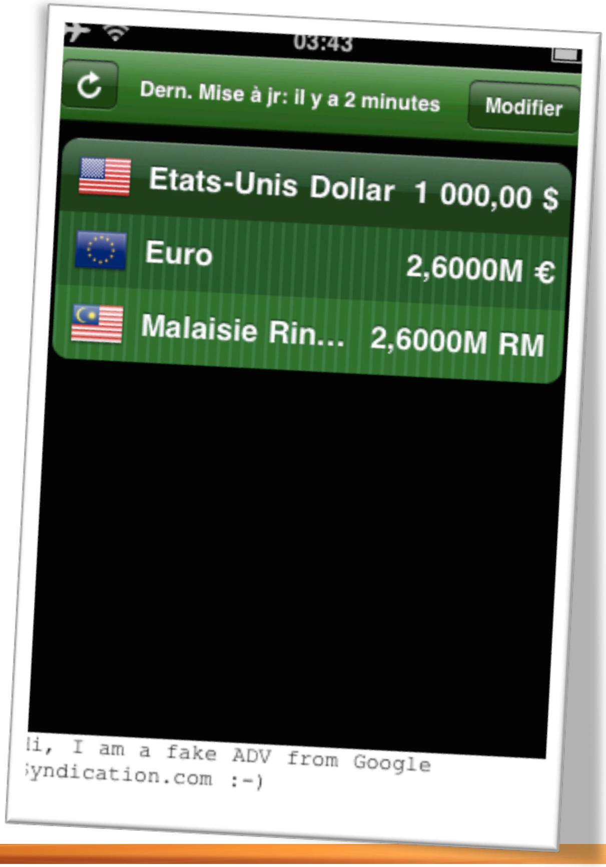


09:07

Dern. Mise à jr: Maintenant

Etats-Unis Dollar	1 000,00 $
Euro	808,30 €
Malaisie Rin...	3 234,00 RM

Trading
www.binck.fr/bourse
Annonces Google



03:43

Dern. Mise à jr: il y a 2 minutes

Etats-Unis Dollar	1 000,00 $
Euro	2,6000M €
Malaisie Rin...	2,6000M RM

```
li, I am a fake ADV from Google
yndication.com :-)
```

WHAT ABOUT THE IPHONE ?

MaxOS X CFNetwork API

- Many applications using network capabilities use this powerfull API
- Examples (check the User-Agents)
  - Facebook/3.12 CFNetwork/459 Darwin/10.0.0d3
  - LinkedIn/3.1 CFNetwork/459 Darwin/10.0.0d3
  - Twitterrific/2.1.6 CFNetwork/459 Darwin/10.0.0d3
  - …
- Reference:

  iPhone OS Reference Library

  - http://developer.apple.com/iphone/library/documentation/networking/conceptual/cfnetwork/

About iPhone applications

- Apple / June 7, 2010
  - Available apps: 225,000+
  - Downloads to date: 5,000,000,000+
  - !!!

- Question ?
  - What if there would be a vulnerability in a low level library shared by thousands of applications ?
    - For blackhats, it would be « insanely great »
- So, we’ve been conducted a kind of pentest on the device, with special fuzzing, etc

CFNetwork: CVE-2010-1752

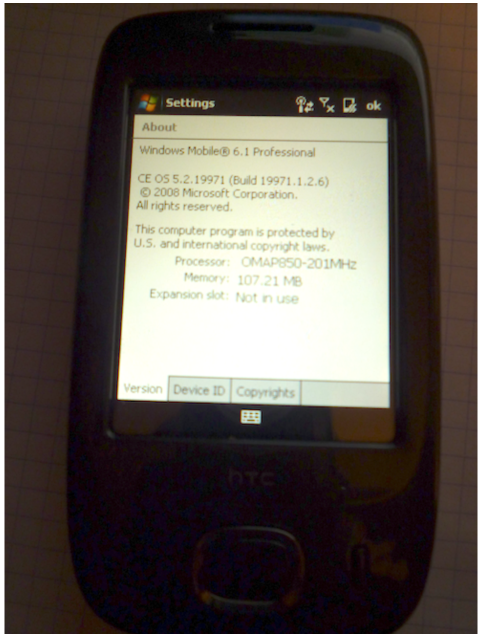
- Reference: http://support.apple.com/kb/HT4225
- Advisory: **TEHTRI-SA-2010-003**

- Devices:
  - iOS 2.0-3.1.3 for iPhone 3G and later,
  - iOS 2.1-3.1.3 for iPod touch (2nd generation) and later
- 0day: Stack overflow in CFNetwork's URL handling code. Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution.
- Solution:
  - Improved memory handling.
- *« Credit to Laurent OUDOT of TEHTRI-Security for reporting this issue. »*
- Apple easily handled the problem as soon as they could (update your iPhone to OS 4.0 now !)

WHAT ABOUT HTC ?

Advisory: TEHTRI-SA-2010-028

- 0day for Opera on HTC devices
  - "HTC_Touch_Viva_T2223 Opera/9.50 (Windows NT 5.1; U; en)"



Settings

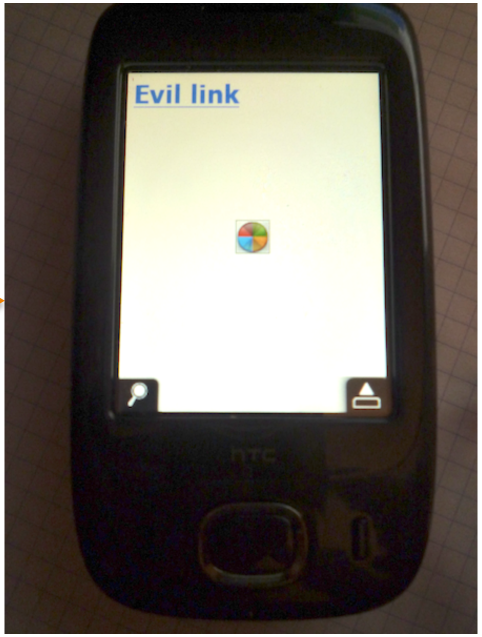
About

Windows Mobile® 6.1 Professional

CE OS 5.2.19971 (Build 19971.1.2.6)
© 2008 Microsoft Corporation.
All rights reserved.

This computer program is protected by U.S. and international copyright laws.

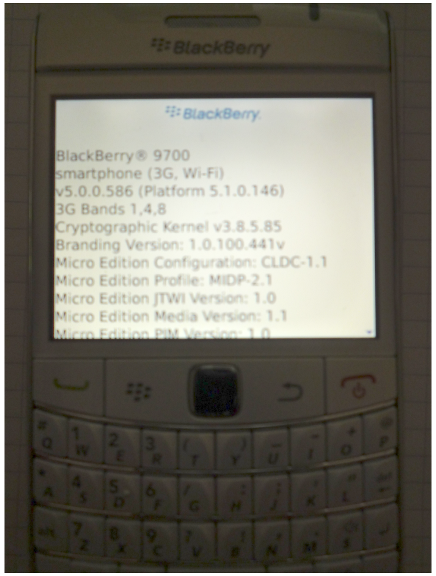
Processor: OMAP850-201MHz
Memory: 107.21 MB
Expansion slot: Not in use



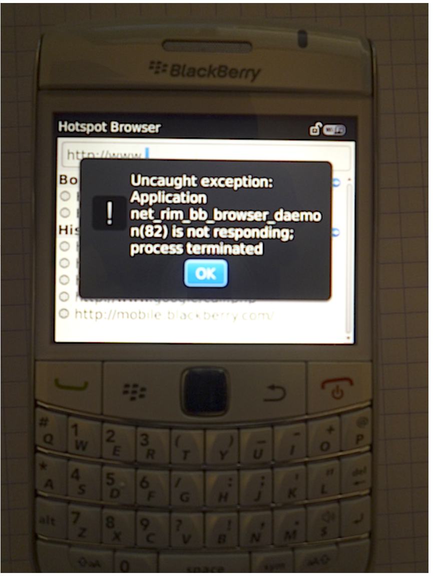
WHAT ABOUT BLACKBERRY ?

Advisory: TEHTRI-SA-2010-027

- 0day for Hotspot Browser on BlackBerry
  - "BlackBerry9700/5.0.0.586 Profile/ MIDP-2.1 Configuration/CLDC-1.1 VendorID/100"



BlackBerry® 9700
smartphone (3G, Wi-Fi)
v5.0.0.586 (Platform 5.1.0.146)
3G Bands 1,4,8
Cryptographic Kernel v3.8.5.85
Branding Version: 1.0.100.441v
Micro Edition Configuration: CLDC-1.1
Micro Edition Profile: MIDP-2.1
Micro Edition JTWI Version: 1.0
Micro Edition Media Version: 1.1
Micro Edition PIM Version: 1.0



Hotspot Browser

http://www.

Uncaught exception: Application net_rim_bb_browser_daemon(82) is not responding; process terminated

OK

http://mobile.blackberry.com/

RIM / BlackBerry

- BlackBerry Security Response Team answered to any of our emails in a really short period of time
- Speed++
  - They handled the security issues & did a great investigation
  - Development of a fix very quickly for a future release
- Not a too big issue: CVSS = 5/10

WHAT ABOUT THE IPAD ?

Advisory: TEHTRI-SA-2010-026

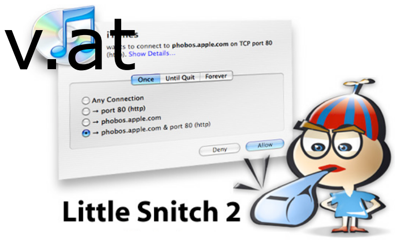
- 0day: Safari, etc, on the iPad
  - "Mozilla/5.0 (iPad; U; CPU OS 3_2 like Mac OS X; fr-fr) AppleWebKit/531.21.10 (KHTML, like Gecko) Version/4.0.4 Mobile/7B367 Safari/531.21.10"

LIVE DEMO

CONCLUSION

Some solutions

- Local Firewall to control unwanted outbound (unknown ?) traffic that could become dangerous
  - e.g: MacOSX: LittleSnitch / www.obdev.at



iTunes

wants to connect to **phobos.apple.com** on TCP port 80 (http). Show Details...

○ Any Connection
○ → port 80 (http)
○ → phobos.apple.com
● → phobos.apple.com & port 80 (http)

- Avoid dangerous areas/networks
- Use safe communications
  - At least, force security !
    - EFF: https://www.eff.org/https-everywhere
- Use safe environments (if any?)
- Update the products
- Contact vendors to switch to SSL…
- Be lucky ☺

Conclusion

- For years, we all knew that MITM issues with HTTP environments are really dangerous.
- But it's 2010 now (!!) and many worldwide web sites + many applications + many devices do not handle MITM threats properly (local client side attacks)
- 0days in the underground + evil activities = tons of problems
- Todo for vendors, companies, etc:
  - Pentest & Harden every sensitive resources with (offensive) experts before the bad guy do it secretly
    - Goals: limit the surface of attack + limit the number of 0days + limit the number of attackers…

“This is not a game.”

Take care. Thanks.

Next Talks & Trainings

- July, China, SyScan HangZhou => 2 talks
- September, Vietnam, SyScan, Training “Advanced PHP Hacking”
- October, Malaysia, HITB, New Training “Hunting Web Attackers”
- November, Austria, DeepSec, Training “Advanced PHP Hacking”
  - First time in Europe !