TEHTRI-Security

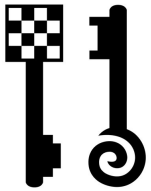
Technology-Ethical-Hacker-Trust-Robust-Information-Security

Inglourious Hackerds Targeting Web Clients

www.tehtri-security.com

INGLØURIOUS HACKERDS

TARGETING WEB CLIENTS

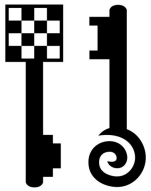


Speaker

- 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 Cansecwest, Pacsec, BlackHat USA-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
  - Advanced & Technical Consulting
  - Penetration Tests / Audits…
  - Fighting Information Leaks, Counter-Intelligence…
- Worldwide:
  - Conferences, Training, Consulting
    - Canada, Lebanon, United Arab Emirates, Singapore, Netherlands, China, Malaysia, France...
  - Press/Media BBC The Register Le Monde LE FIGARO ZDNet
- >30 public security advisories (9 months)
  - Pentesting devices & Applications → 0days…



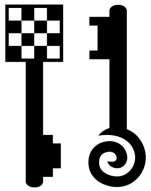
Introduction

- Goal:

  Analyze some techniques used by *inglourious hackerds*, targeting web clients

  Think about solutions

- Target audience:
  - White hats, to fight against Cybercrime, Business Intelligence, Information Warfare
- Notice:
  - Legal Issues: we remind you to carefully respect the laws in your country before applying some techniques shown in this presentation
  - Limitation: this is an almost 1 hour only talk. We won't be able to cover all the related subjects. Contact us for more.



Plan

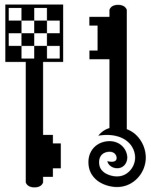
Inglourious Hackerds, Targeting Web Clients

1 – Global Overview

2 – Finding vulnerabilities

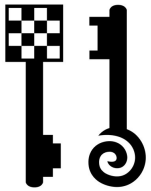
3 – Attacking Web Clients

4 – Conclusion



Let’s have a look at the theory and at some concepts related to attacks against web clients

I. GLOBAL OVERVIEW

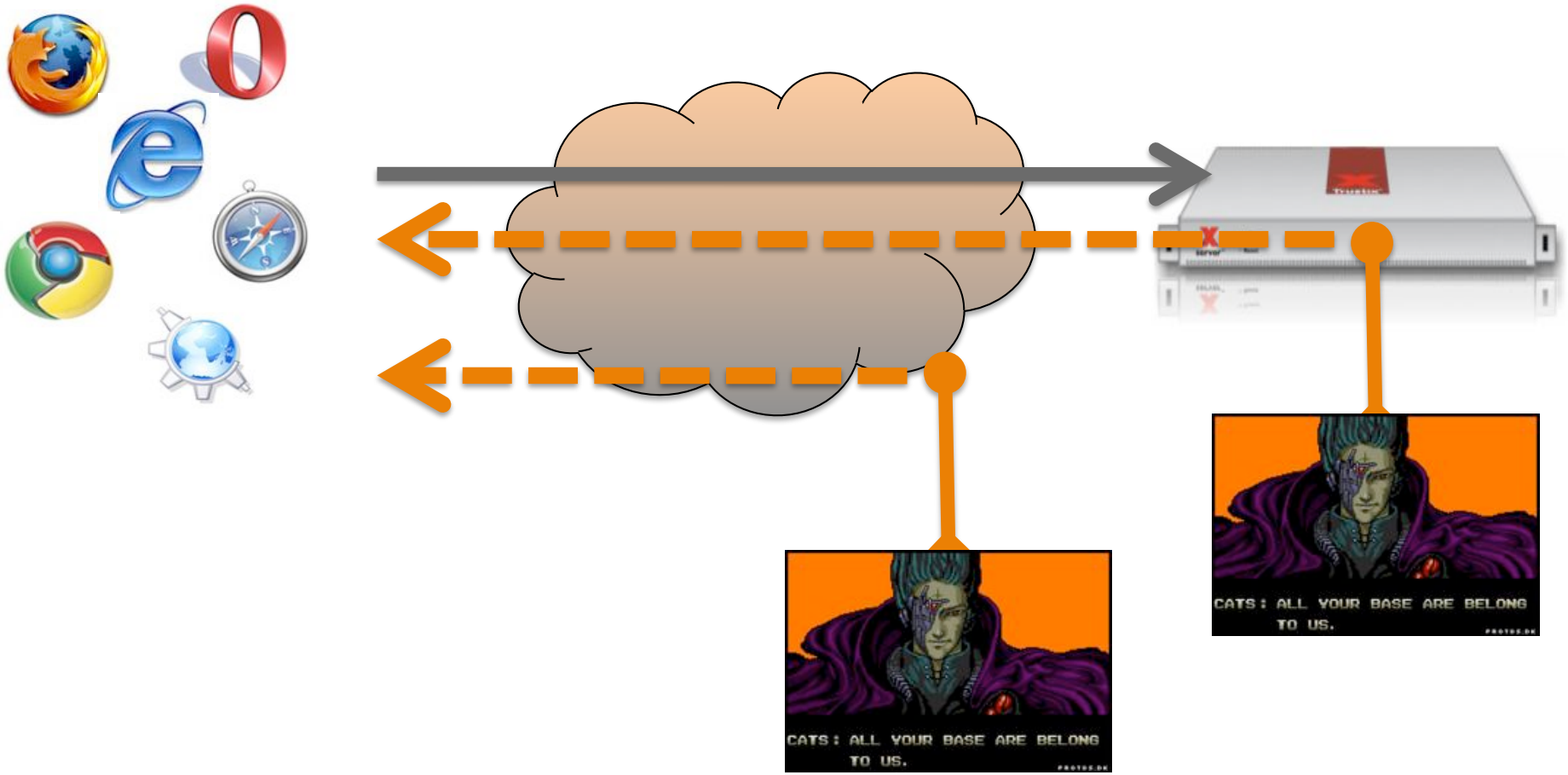


Battlefield: Web Hacking

- Web targets (standard aspects)
  - Web Clients (browsers)
    - Client-side attacks
    - "Human" interaction (at least the beginning)
  - Web Servers (services)
    - Direct attacks
    - Technical interaction
- In this presentation, we'll focus on attacks against **web browsers**, and how inglourious hackerds try to play hard against their targets

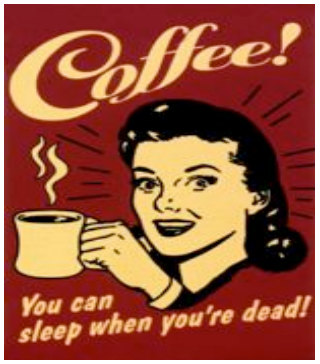
Targeting Web Clients

- Evil responses (Server or MITM)



Example: Wifi threats

Home

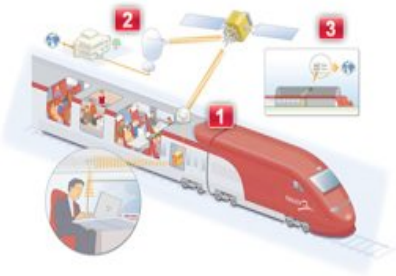


Coffee/Bars

Restaurants

Hotels

Corporate…

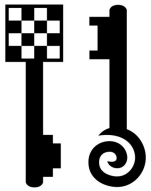


Trains

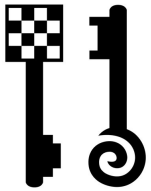
Planes

Bus

Taxis / Cars

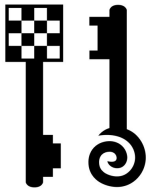


2. FINDING VULNERABILITIES



Finding vulnerabilities

- Reverse
- Fuzzing
- Analyzing behavior (Logs, Sniffing…)
- Audit
- Pentest
- …



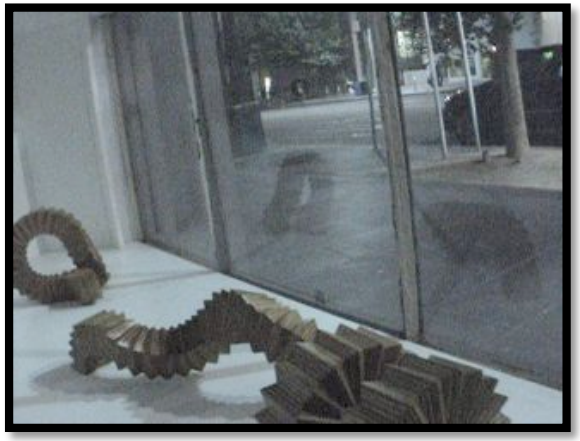
Fuzzing

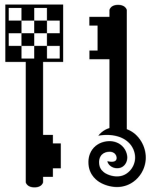
- Sounds easy
- Not that easy
  - Random fuzzing → Sharp fuzzing

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

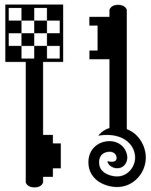
Finding 0days in devices

- E.g.: TEHTRI-Security found a 0day against a widely used IP Camera (Surveillance)

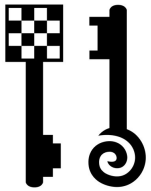


3. ATTACKING WEB CLIENTS

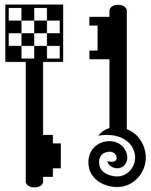


3.1 ANONYMOUS TRANSFERS THROUGH WEB CLIENTS



Anonymous transfers

- Playing with web clients in order to transfer data between web servers
  - Bounces
  - XSRF like concepts
  - 302 Redirections



#1 - First transfer example

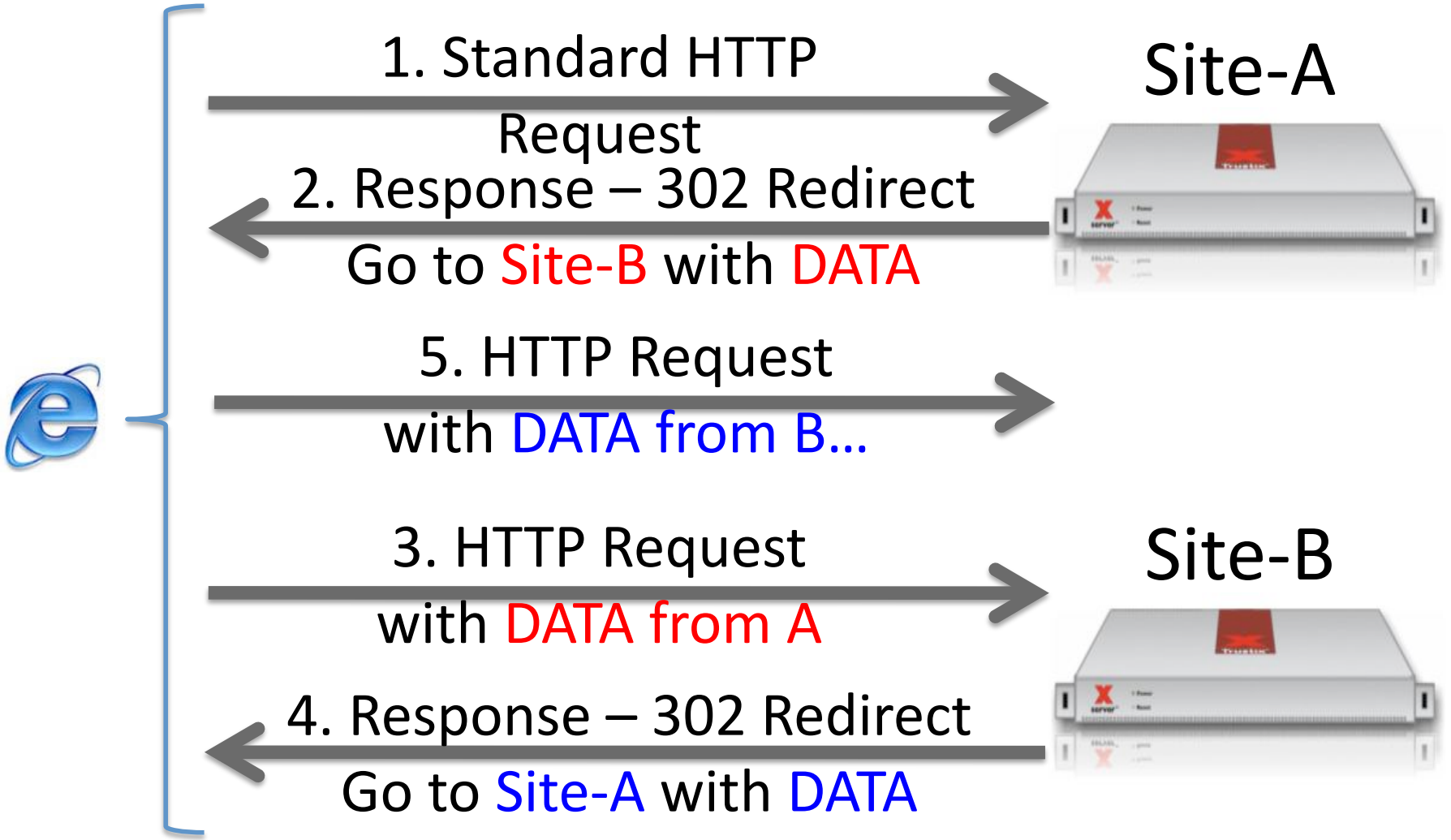
- Site-A wants to transfer data to Site-B without any direct talk between them

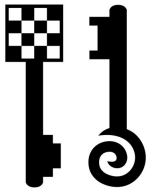
- Tiny solution on Site-A: display a web page to an incoming web client, containing links to Site-B, like:

```
<IMG SRC="http://site-b/foo.asp?
  exchange=data-to-send" width="0" />
```

- More funny with pananoid web clients that delete REFERER HTTP field

#2 - Loop Attack example



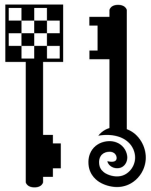


About the 302 HTTP Response

```
HTTP/1.1 302 Found
Date: Thu, 06 Jan 2011 17:31:28 GMT
Server: Apache/2.2.15 (Unix) mod_ssl/
  2.2.15 OpenSSL/0.9.8l DAV/2 PHP/
  5.3.3 X-Powered-By: PHP/5.3.3
Location: http://site-b/
  communication.php?data=XXXXXXXXXX
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

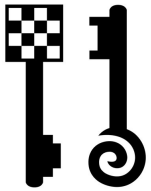
Maximum Number of Loops

- Example with Safari



Optimize with "User-Agent"

Web Browser	Max number of loop messages allowed between Site-A and Site-B
MS Internet Explorer 8	9
Latest Apple Safari	15
Latest Google Chrome	19
Latest Mozilla Firefox	19
…	…
MS Internet Explorer 6	99 (!)

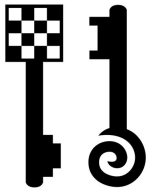


Client-Side Anonymous Transfer

- We saw how to play with web clients in order to transfer data between servers
- If you want to try, you'll need to think about the User-Agent, and the limitation of size through a GET (with 302)
- There also exists other fields of research in order to place Data
  - REFERER
  - COOKIES

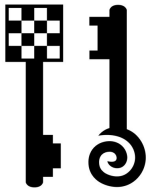
One vulnerability to rule them all

3.2
EXPLOITING *MANY* WEB CLIENTS



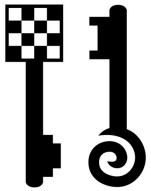
RTFM: RFC

- RFC 2396 « Uniform Resource Identifiers (URI): Generic Syntax »
- RFC 2616 « Hypertext Transfer Protocol -- HTTP/1.1 »
  - The HTTP protocol does not place any a priori limit on the length of a URI. Servers MUST be able to handle the URI of any resource they serve, and SHOULD be able to handle URIs of unbounded length if they provide GET-based forms that could generate such URIs.
  - A server SHOULD return 414 (Request-URI Too Long) status if a URI is longer than the server can handle (see section 10.4.15).



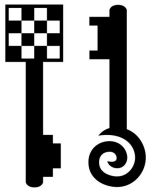
Exploit ?

- According to RFC: no limit to the size of a URI
- Reality: practical limits on the available resources
  - Solution: limitations fixed by vendors
    - Example:
      - http://support.microsoft.com/kb/208427
      - Maximum URL length is 2,083 characters in Internet Explorer
- Special case: mobile devices
  - Limited resources
  - Special analysis of HTML
    - Dynamic interpretation of phone numbers, dates, etc



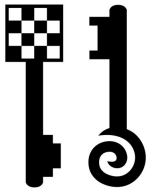
Example of Security Issue

- Handled devices
- Analyzing HTML content
  - Make decisions about how to process a link based on its structure and makeup
  - Designed with typical/average length URIs
  - Consists of walking through the URI several times, performing comparisons and trying to extract things such as email addresses or phone numbers
  - Then it might need to launch appropriate external application (email composer, sms editor, etc)

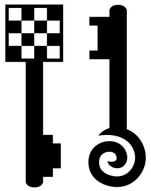


What if ?

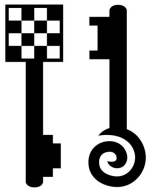
- Security issue
  - Extremely long URI provided with evil links
  - Parsing takes up a considerable amount of resources (typically, memory and CPU cycles) and the web client is unresponsive while it waits for the parsing to complete
- Watchdog mechanism detects that a process is stuck or otherwise unresponsive
- Error message displayed and/or crash
  - Sometimes it's not descriptive from an end user's perspective but it is accurately stating what has happened
  - The web client process or other processes or the device, might terminate because it has stalled



EXPLOIT(S) ?



HTC PRODUCTS

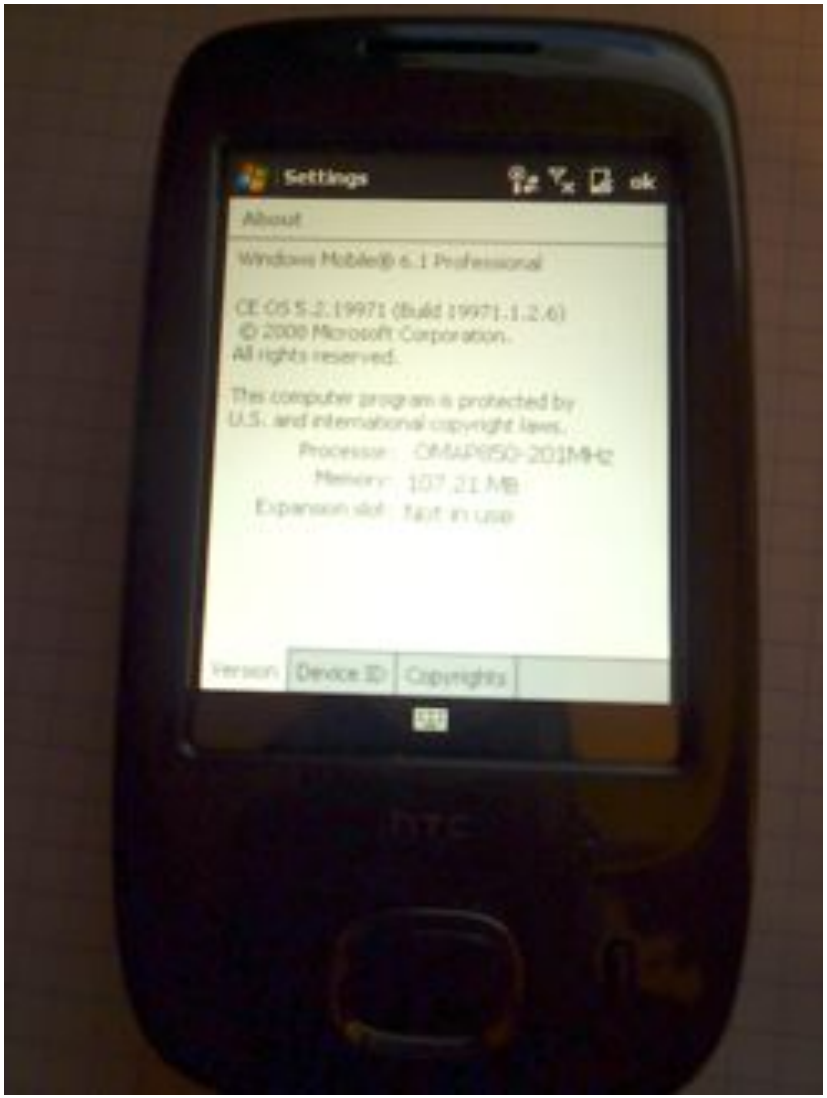


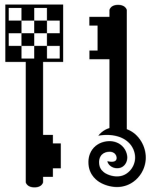
Security Issue Found

- Client-side attack with at least a remote crash of the browser and / or the device

Products affected

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





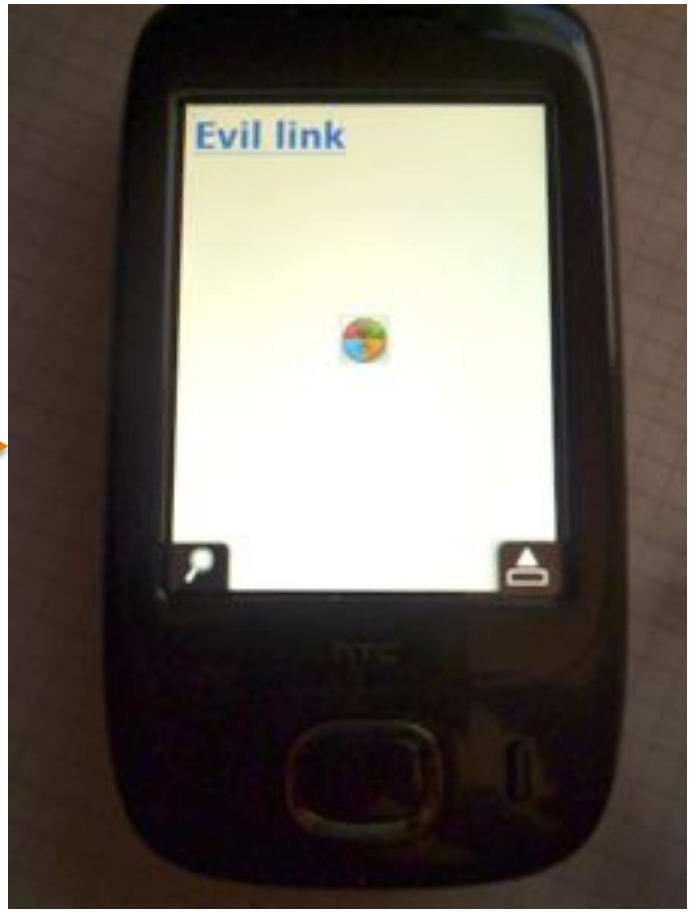
Vendor responses

- Advisory sent with exploit code (0day)
  - June 2010

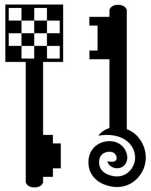
- Official response of the vendor:
  - « Kindly provide us with the correct IMEI or Serial Number of your handset for further assistance »

Technical details

- Advisory: TEHTRI-SA-2010-028

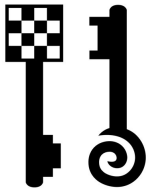


APPLE PRODUCTS



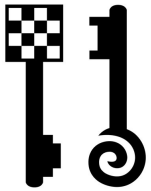
Security Issue Found

- Stack overflow in CFNetwork's URL handling code
  - Low layer found in many Apple products
- Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution



Products affected

- Safari on Windows
- Safari on Mac OS X
- CFNetwork on iPod
- CFNetwork on iPhone

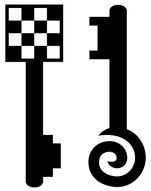


Vendor responses

- Discussions
  - First advisories in 2010
- Patches
  - Improved memory handling
- CVE-2010-1752
  - iPod
  - iPhone (patch with iOS 4)
  - Safari Windows
  - Safari MacOSX and MacOSX Server

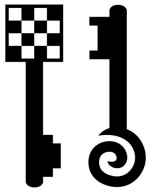
Another trick

- iPad Advisory: TEHTRI-SA-2010-026
  - Watchdog crash due to low memory conditions (not related to CFNetwork)
  - Cannot be exploited to execute arbitrary code. Fixed in a future software update.



E.g. Safari on Windows

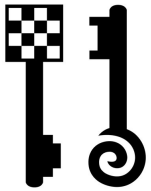
- Sun Feb 22 02:03:36.570 2010 (UTC + 2:00): (e70.a84): Stack overflow - code c00000fd (first chance)
- First chance exceptions are reported before any exception handling. This exception may be expected and handled.
- eax=00032000 ebx=0c3e0020 ecx=00000000 edx=027b2060 esi=0c3e0020 edi=055d4aae eip=017a80d7 esp=0012f10c ebp=0012f12c iopl=0 nv up ei pl nz na pe nc cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010206
- Loading symbols for 01750000 C:\Program Files\.... \Apple\Apple Application Support\CFNetwork.dll
- CFNetwork!CFURLProtocolSendDidFinishLoadingCallback +0x6056: 017a80d7 8500 test dword ptr [eax],eax ds: 0023:00032000=00000000
- Loading symbols for 01f90000 C:\Program Files\.... \Apple\Apple Application Support\WebKit.dll



E.g. Safari on MacOSX

```
Process:         Safari [3254]
Path:            /Applications/Safari.app/Contents/MacOS/Safari
Identifier:      com.apple.Safari
Version:         5.0.2 (6533.18.5)
Build Info:      WebBrowser-75331805~1
Code Type:       X86-64 (Native)
Parent Process:  launchd [3178]
OS Version:      Mac OS X 10.6.4 (10F569)
Crashes Since Last Report:          1739
Exception Type:  EXC_BAD_ACCESS (SIGSEGV)
Exception Codes: KERN_PROTECTION_FAILURE at 0x00007fff5df61b38
Crashed Thread:  0  Dispatch queue: com.apple.main-thread
...
Thread 0 Crashed:  Dispatch queue: com.apple.main-thread
0   com.apple.CFNetwork               0x00007fff859a9686 URLResponse::copySuggestedFilename() + 806
1   com.apple.Foundation              0x00007fff80e7c352 -[NSURLResponse suggestedFilename] + 31
2   com.apple.WebCore                 0x00007fff84d0d26b WebCore::ResourceResponse::platformLazyInit() + 475
3   com.apple.WebCore                 0x00007fff84d86b91 WebCore::ResourceResponseBase::httpStatusCode() const +
17
4   com.apple.WebCore                 0x00007fff84d91e25
WebCore::ApplicationCacheHost::maybeLoadFallbackForResponse(WebCore::ResourceLoader*, WebCore::ResourceResponse
const&) + 37
5   com.apple.WebCore                 0x00007fff84d91d43 WebCore::ResourceLoader::didReceiveResponse
(WebCore::ResourceHandle*, WebCore::ResourceResponse const&) + 67
...
Thread 0 crashed with X86 Thread State (64-bit):
  rax: 0x0000000001c9c390  rbx: 0x00000001194e43b8  rcx: 0x00007fff7118e3e0  rdx: 0x0000000001c9c390
  rdi: 0x000000012c089000  rsi: 0x00007fff5df61b40  rbp: 0x00007fff5fbfdf50  rsp: 0x00007fff5df61b40
   r8: 0x00007fff85a0fd3e   r9: 0x0000000000000000  r10: 0x00000001008aa750  r11: 0x00007fff5fbfde80
  r12: 0x000000012c089000  r13: 0x0000000117601de0  r14: 0x0000000100af4900  r15: 0x00007fff84d91d00
  rip: 0x00007fff859a9686  rfl: 0x0000000000010202  cr2: 0x00007fff5df61b38
```

RIM PRODUCTS

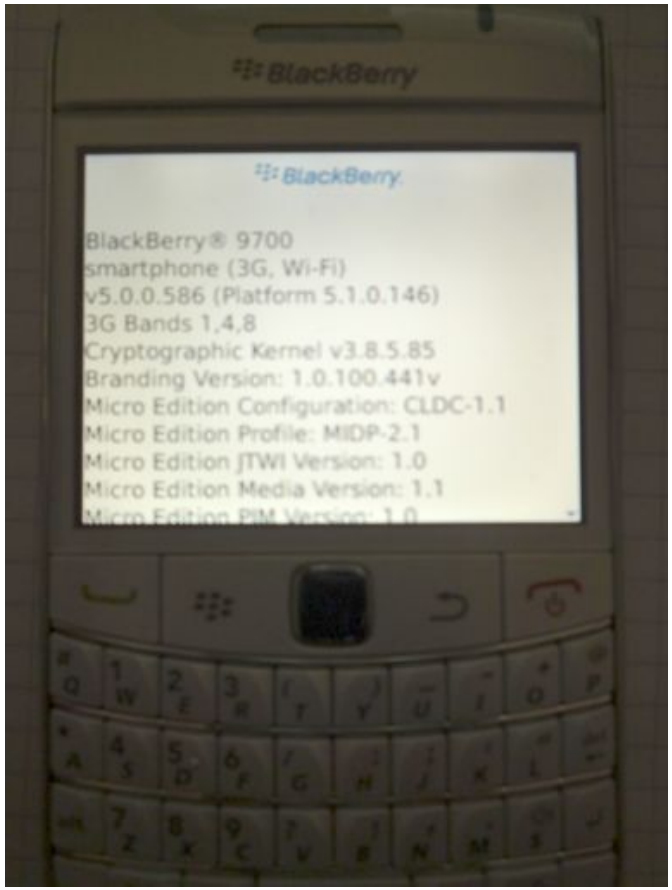


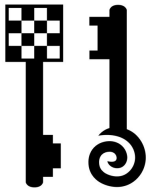
Security Issue Found

- Maliciously crafted web page viewed by a vulnerable BlackBerry → the browser application becomes unresponsive
- The BlackBerry device subsequently terminates the browser, and the browser eventually restarts and displays an error message.
- Successful exploitation of this issue relies on the user viewing the maliciously crafted web page on a device running the affected BlackBerry Device Software.
- The impact is limited to a partial Denial of Service (DoS) in the browser application in use on the BlackBerry device

Products affected

- The issue affects the BlackBerry browser application of the following software versions:
- BlackBerry Device Software versions earlier than 6.0.0
- Hotspot Browser on BlackBerry
  - "BlackBerry9700/5.0.0.586 Profile/MIDP-2.1 Configuration/ CLDC-1.1 VendorID/100"



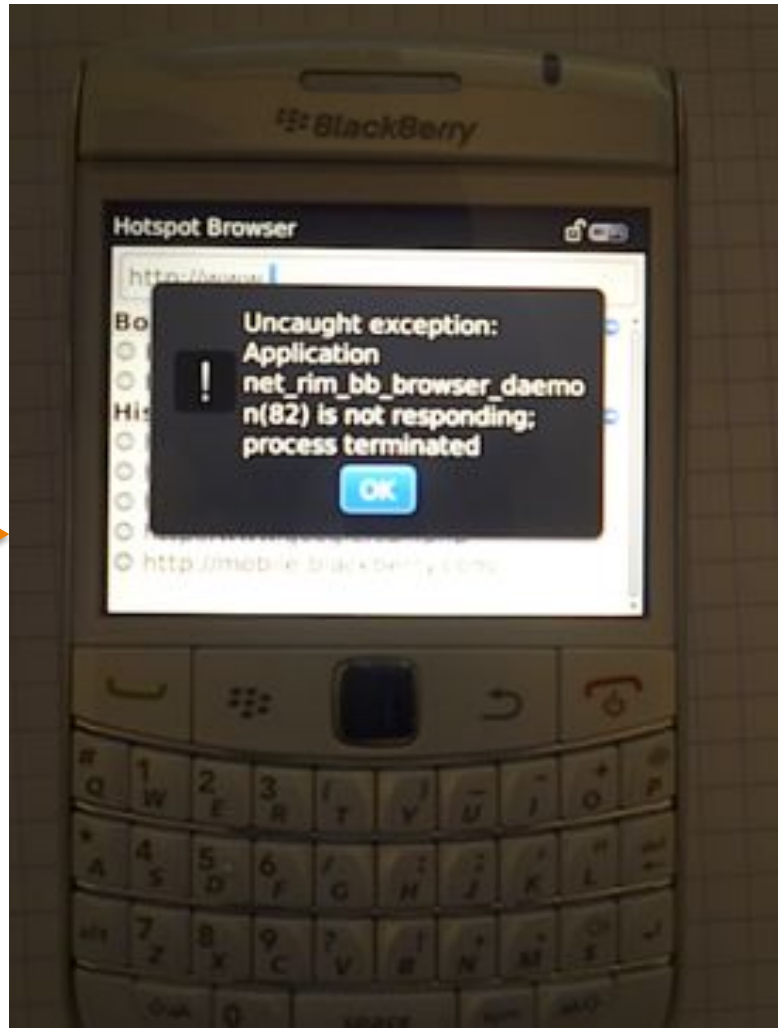


Vendor responses

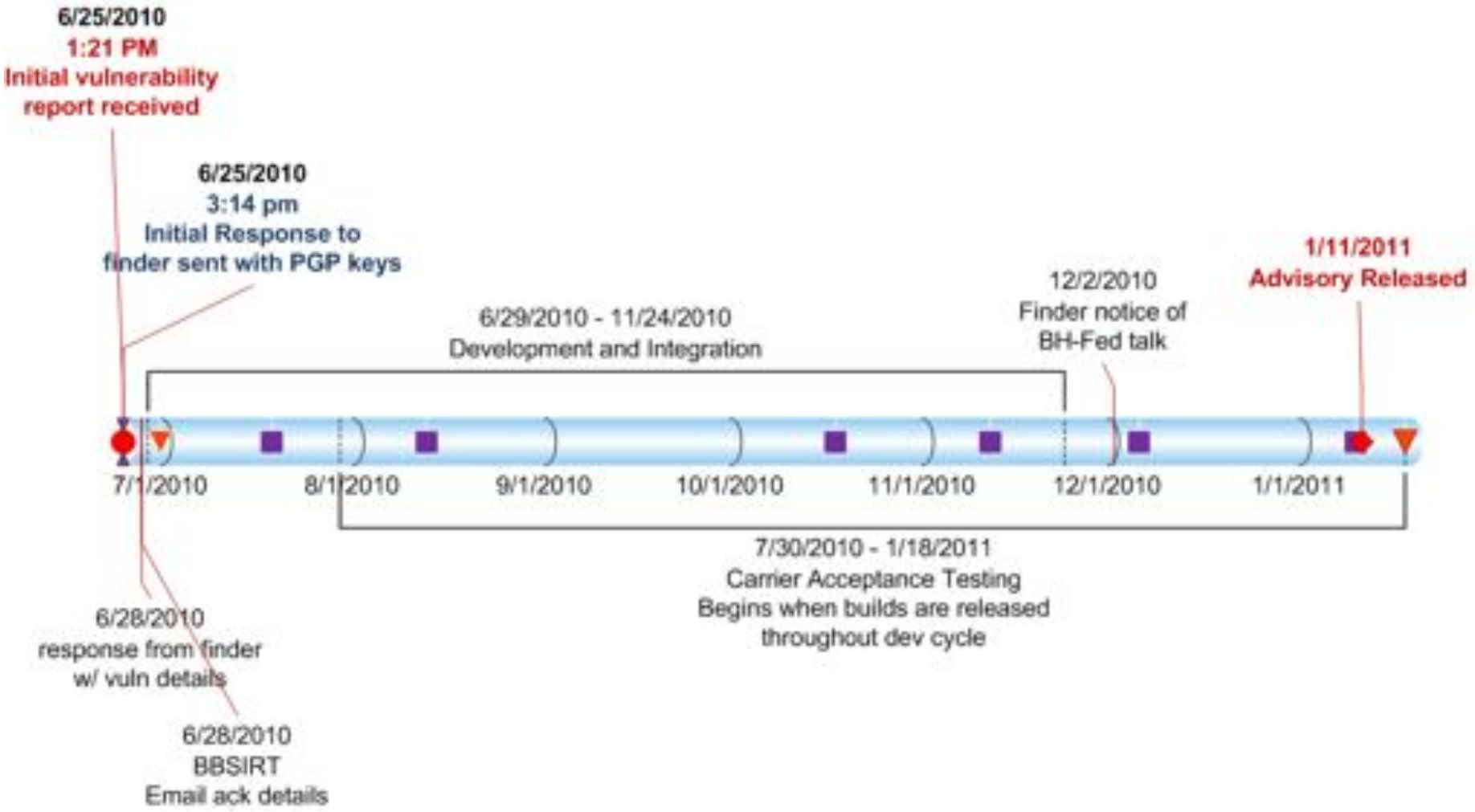
- RIM has issued a software update that resolves this issue in BlackBerry Device Software versions later than 5.0.0. BlackBerry Device Software version 4.7.0 and earlier is unsupported, and versions later than 6.0.0 are unaffected.
- BlackBerry Security Response answered to any of our emails in a really short period of time
- Speed++
  - They handled the security issues & did a great investigation
  - Development of a fix very quickly for future releases + Patch for old products
- CVSS: 5/10

Technical details

- CVE-2010-2599
- TEHTRI-SA-2010-027



Timeline


6/25/2010
1:21 PM
Initial vulnerability report received
6/25/2010
3:14 pm
Initial Response to finder sent with PGP keys
6/29/2010 - 11/24/2010
Development and Integration
12/2/2010
Finder notice of BH-Fed talk
1/11/2011
Advisory Released
7/1/2010
8/1/2010
9/1/2010
10/1/2010
11/1/2010
12/1/2010
1/1/2011
7/30/2010 - 1/18/2011
Carrier Acceptance Testing
Begins when builds are released throughout dev cycle
6/28/2010
response from finder w/ vuln details
6/28/2010
BBSIRT
Email ack details

Opportunities / Challenges

Challenges

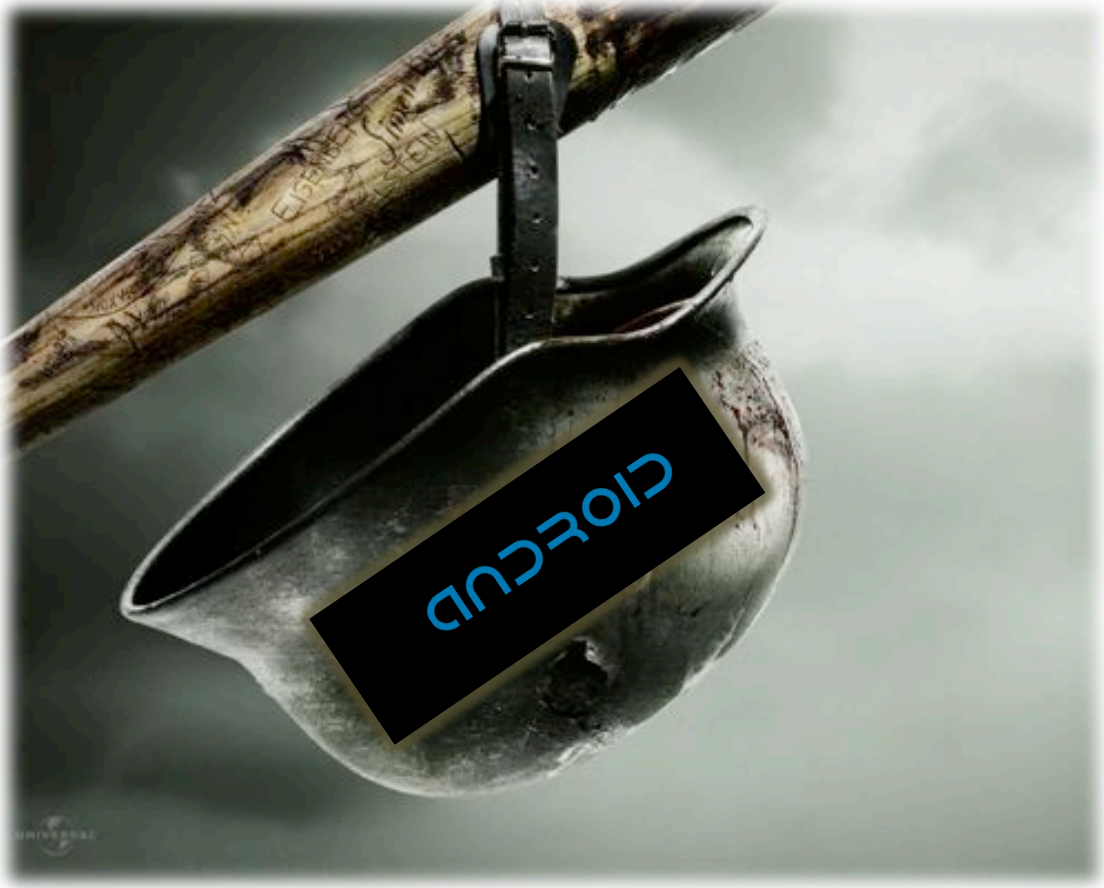
- Response Muscle Memory
- Product Diversity
- Servicing complexity
- Fix Delivery

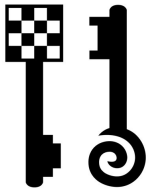
Opportunities

- BBSIRT SME for Handheld issues
- Handheld servicing strategy
- Carrier relationships
- Internal relationships

secure@blackberry.com
www.blackberry.com/security

GOOGLE PRODUCTS



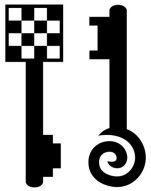


Security Issue Found

- Overflow against application Browser on Android with large input from the web

- Overflow against application Gmail on Android with large input from the web

  e.g: « Gmail is prone to a vulnerability after being launched by Browser trying to handle some web pages that would contain specific evil code. »

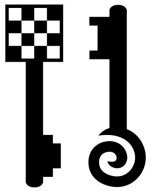


Products affected

- Firmware tested: 1.5
- Kernel version tested: 2.6.27
- User-Agent tested:
  « Mozilla/5.0 (Linux; U; Android 1.5; en-us; GT-I5700 Build/CUPCAKE)
  AppleWebKit/528.5+ (KHTML, like Gecko) Version/3.1.2 Mobile Safari/525.20.1 »

- Name: Gmail (com.google.android.gm)
  Activity: Compose (application Gmail)

- Name: Browser (com.android.browser)

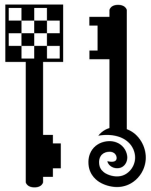


Vendor responses

ANDROID

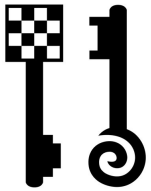
- « Traditionally, we do not consider local denial of service attacks of this kind to be security bugs. »

- No patch needed ☺



Proof of Concept #1

This slide was only shared during BlackHat DC 2011



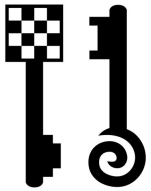
Technical details #1

ANDROID

This slide was only shared during BlackHat DC 2011

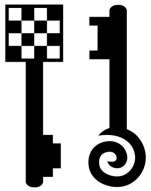
Screenshots #1

- Overflow against application Browser on Android with large input from the web



Proof of Concept #2

This slide was only shared during BlackHat DC 2011



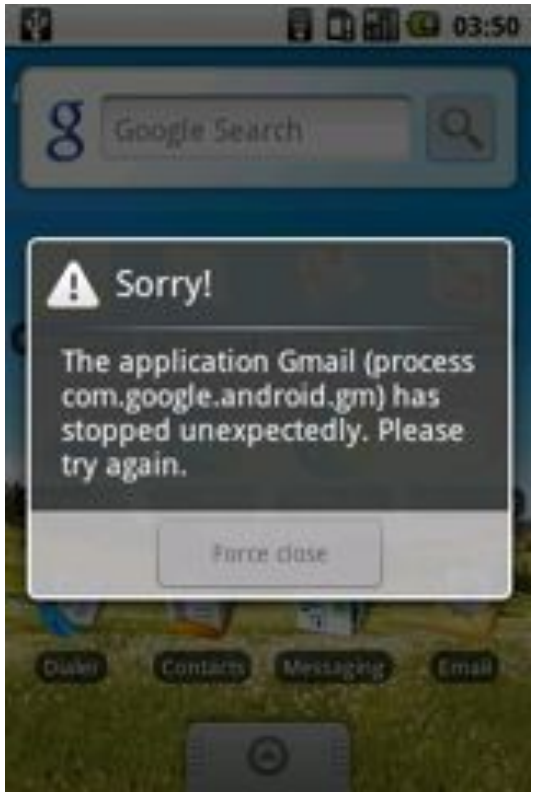
Technical details #2

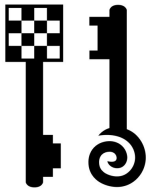
ANDROID

This slide was only shared during BlackHat DC 2011

Screenshots #2

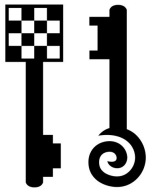
- Overflow against application Gmail on Android with large input from the web





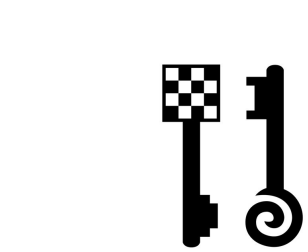
Found by TEHTRI-Security [2010]

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	?	?

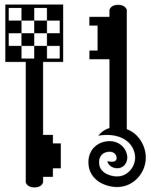


Is that a security threat ?

- Those attacks can be used by combining different techniques
  - Mail: Imagine evil links sent by email directly with pointers to bad servers
  - MITM: Imagine a wireless hotspot with someone running all those exploits for any vulnerable devices?
    - Crash of vulnerable devices… (massive pwnd/DoS)
    - You could also add another trick:
      - 1st you crash the clients,
      - 2nd you display a fake security web page for phishing, etc
        - » *Vendor message: your device just crashed and we need to re-enroll your account for your security, please fill in the form…*
- Other vendors? ☺

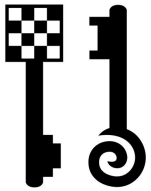


3.3 COUNTER-STRIKE



Fighting against those tools ?

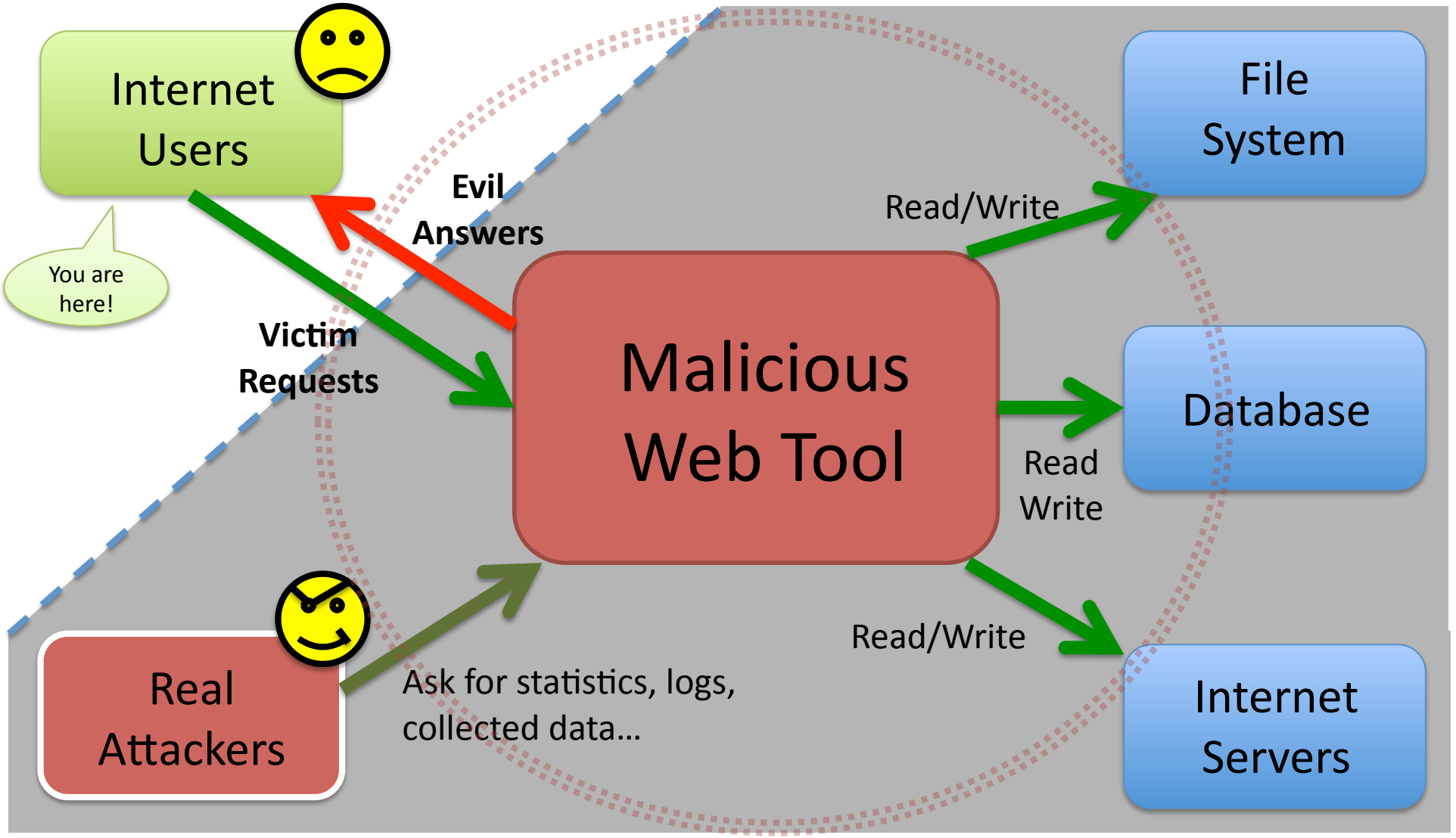
- In the past, I explained how to strike back against some evil tools:
  - Black Hat Singapore 2003: « Honeypots against Worms 101 »
    - http://www.blackhat.com/presentations/bh-asia-03/bh-asia-03-oudot/slides/bh-asia-03-oudot.pdf
  - « Fighting Internet Worms With Honeypots », 2003
    - http://www.symantec.com/connect/articles/fighting-internet-worms-honeypots
  - Defcon 12, Las Vegas 2004: « Digital Active Self Defense »
    - http://www.defcon.org/images/defcon-12/dc-12-presentations/Oudot/dc-12-oudot-up.pdf
  - CanSecWest, Vancouver 2004: «Towards Evil Honeypots ?! When they bite back »
  - ...

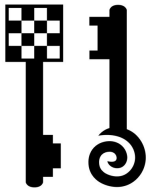


Malicious Web Activities

- What is commonly done by evil people once they exploit web servers ?
  - Control the owned box : Add a backdoor / bounce tool / remote exploration tool…
  - Use the owned box to attack incoming clients with "Client-Side Attacks" (Aurora…)
  - Use the owned box to abuse incoming clients with "Pharming Attacks" (phishing…)
  - Store malware to use the owned box as an evil resource repository (malware distribution, RFI, Command & Control for Backdoors…)

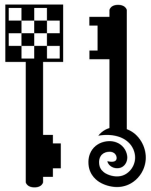
Interaction of those tools





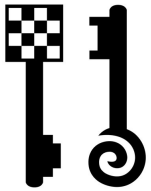
Striking Back ?!

- How to strike back ?
  - Build requests from web clients that will exploit the remote system
  - Find security flaws in the remote administration system used by the attackers to monitor the tools
  - Find unprotected interesting resources
- What to target ?
  - Web vulns
  - File System issues
  - Database issues
  - Remote administration issues
  - …



White-Box Strike Back

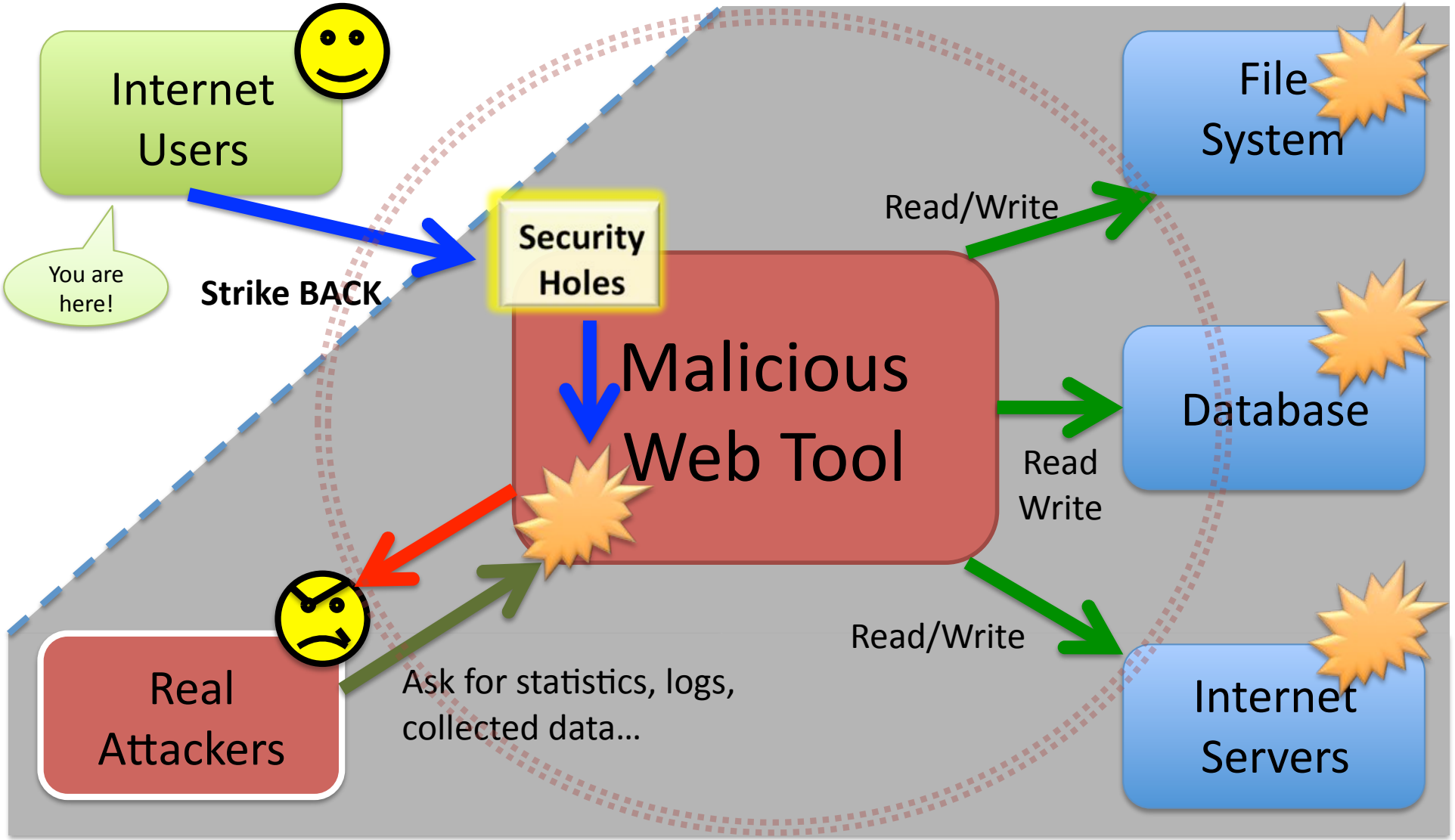
- You have details about the remote malicious web tool used by the attackers
  - Name of Product, Version…
- You have / find / buy the sources of the remote tool
  - Audit the source code and the tool
  - Find vulnerabilities
  - …

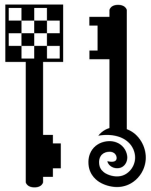


Black-Box Strike Back

- You have no detail about the remote malicious web tool deployed
- It's a black box hacking attempt against the attackers
- More complex (unless you can switch to white-box)
- What helps ?
  - Same vulnerabilities found on different products because of code shared/stolen
  - You don't attack a real target, but you attack a compromised (?) computer used as a bounce, so that their might be less monitoring regarding your intrusion tests (no NIDS, etc, used by the attackers)
  - Black Hats find vulnerabilities on known products, but they don't really audit their own sources ☺
  - ...

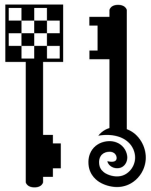
Hack back needed parts





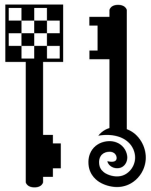
Gather information about attackers

- Each time the attackers connect back to their administration backend on the malicious web tool (to get statistics, to control their tools…), they take risks
- Once you can modify some data on the remote web tool used by the attackers, you can inject specific code to :
  - Get their real IP addresses, info, etc
  - Fight back (client-side attack against the attackers themselves !)



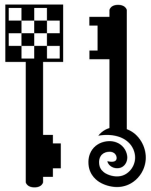
Getting info about standard attackers

- Standard attackers won't use proxies, etc, to connect back to the administration backend of their malicious web tools
- You can easily inject code to get more info about them, even if you don't have access to the remote HTTP logs
- Examples
  - Add <img src= to force an HTTP traffic from the attacker, to a monitored web server…



Getting info about stealth attackers

- Some attackers might try to use proxies, so that you'll have to try to abuse some of their plugins
- Java
  - Inject code that will try RAW TCP and UDP sockets. You might see incoming traffic on a monitored resource (works with old JRE on MacOSX for example)
- Quicktime
  - Embedded MOV
- Windows Media (Flip4Mac on MacOSX)
  - HREF="mms://…"
- Shockwave
  - Use flash.net.XMLSocket to open sockets with XMLSocket()
- …



Attack the attackers

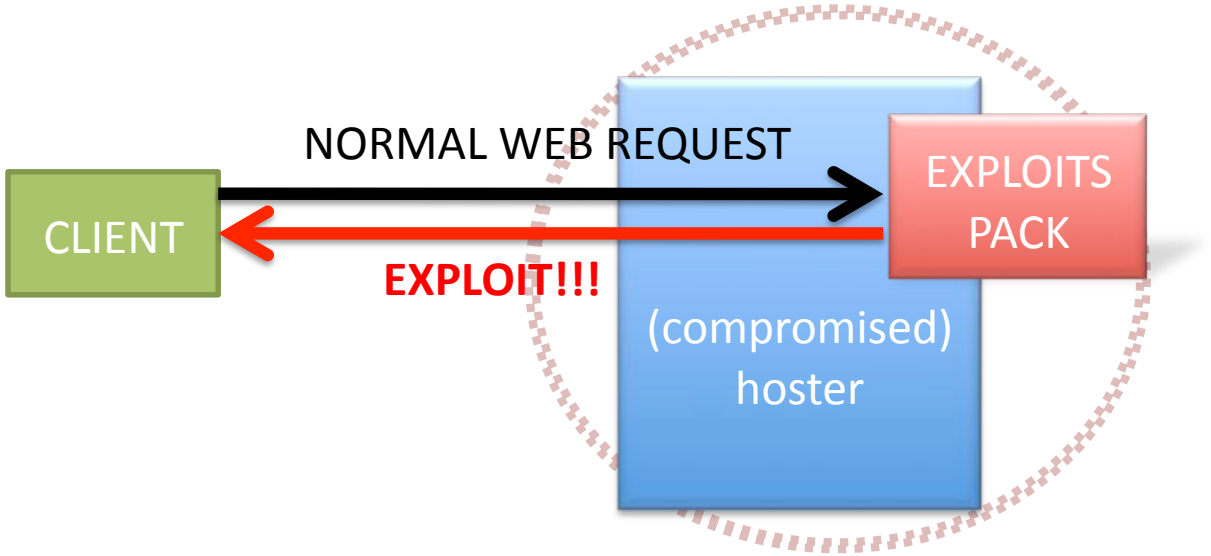
- In such cases, when you want more than information about the attackers, you might want to attack them back
- You'll need to know their tools and methods, to adapt your response and inject it through their interactions with their evil web tools
- Most of the time, it's a like dealing with "client side" attack for the web tech
- The content replied by the compromised web server has to become evil when needed

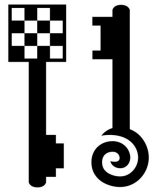
Example: Exploit Kit "SpyEye"

- Evil trojan used to steal sensitive information

About exploits packs / kits

- Automatic Client Side Attacks
  - Each incoming web client is attacked back
  - It first analyze the User-Agent, plugins, etc
  - Then it launches the exploits
  - Offers statistics, control, etc, to the attackers
- Public (first?) known example: MPACK





Eleonore exploit pack

- Price USD 700
- Builtin exploits
  - MDAC
  - MS009-02
  - Telnet – Opera
  - Font tags – FireFox
  - PDF collab.collectEmailInfo
  - PDF collab.getIcon
  - PDF Util.Printf
  - DirectX DirectShow
  - Spreadsheet

Attack the SQL statistics

- **TEHTRI-SA-2010-012 Eleonore: SQL Injection as a fake web victim**
- **[0day]**

This slide was only shared during BlackHat DC 2011

Example of exploit

- **TEHTRI-SA-2010-013 Eleonore: permanent XSS against admin panel**
- **[0day]**

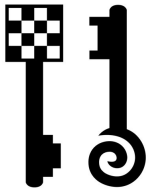
This slide was only shared during BlackHat DC 2011

XSS & XSRF vulnerabilities

- **TEHTRI-SA-2010-014 Eleonore: XSRF in stat.php**
- [0day]…

This slide was only shared during BlackHat DC 2011

Many Exploits Packs……!!



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

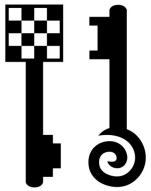
4. CONCLUSION

Situation

- Beyond the technical world, lot of external problems
  - Some believe that products are secured by default
  - But IT infrastructures get more and more complex
  - And we all face money and speed issues…
- So that, many products are used without being stressed or tested
  - Cell phones, VOIP phones, IP Camera…
  - Vulnerabilities (0days) & Offensive concepts
  - Low costs behaviors can cost a lot

Conclusion

- Behavior
  - Being certified ➔ Feeling secure
  - Being certified ≠ Being secure
  - Are your enemies "ethical hackers"?
- What should be done?
  - You saw how easy it was to found multiple web vulnerabilities on widely used products
  - Hardening + (real) Pentest + Analysis
    - Before buying stuff + before & after deployment…



THANKS !

- BlackHat family (Ping…)
- RIM Company (Kymberlee Price, Adrian Stone, Mark Long, Michael McCallum…)
- Apple Folks (@product-security, Matt, Geoff, Mihaela, Jeffrey…)

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