Wireless Hacking Tablet

This document will go into detail configuring Fedora Core 4 on a Motion Computing m1300 tablet for wireless sniffing, encryption hacking, and client hijacking.

NOTE: *Only the madwifi-old drivers and kernel in Fedora Core 4 works with the wireless client expoitation framework Karma.*

This document will detail installation of both Fedora and Windows XP tablet edition in a dual-boot environment to take advantage of Windows wireless tools as well (i.e. AirMagnet).

Download and burn to disk the 4 cd iso files or 1 dvd iso file from www.fedora.org. I find the dvd a lot easier as you don't have to constantly swap disks. When installing the operating system we will make changes to the disk partitioning to allow unused space for Windows XP. Additionally we will customize the installation of software packages to ensure we have all the tools we need to install the wireless security utilities.

Choose Language [English]
Choose Keyboard [U.S. English]
Choose Installation Type [Custom]
Disk Partitioning [Manual Disk Druid]

Delete all partitions identified. Fedora likes to default to disk volumes. This will be fine if you know what you are doing. I'm not totally comfortable with volume disks and still prefer old style partitioning so that is how I will configure it. Remember we want to leave space for the Windows install.

The tablet has a 40GB harddrive and 1GB of ram. I will give 15GB for the Windows install and partition the remaining 25GB as follows.

500mb /dev/hda1 mounted to /boot formatted ext3
23000MB /dev/hda2 mounted to / formatted ext3
1500MB /dev/hda3 mounted as swap

Boot Loader Config [default]
Network Config [default] – It will configure the Ethernet interface (eth0) with dhcp.
Firewall Config [disabled]

we will disable the firewall and SELinux. This is a hacking device and these options will interfere or hamper what we want to do.

TimeZone [Eastern]
Set Root Password [assign your password]

Packages
X Window System [defaults]
Gnome Desktop Environment [defaults]
Editors

Vim-enhanced
Emacs [if you prefer]
Graphical Internet
Firefox
Text-based Internet
Elinks
Lynx
Office/Productivity
[defaults] for open office
Xpdf
Server Configuration Tools [select all]
Web Server [select and keep defaults]
Windows File Server [select all]
DNS Name Server [select all]
Network Servers
dhcp
Development Tools [select, keep defaults, but add: Ruby, svn, and expat]
Language Support [deselect]
Administration Tools [select all]
System Tools [select and from defaults remove nmap]
Printing Support [default]

Welcome
License Agreement [agree]
Date and Time [configure]
Display [Configure]
Monitor->Generic LCD Display->LCD Panel 1024x768
Resolution->1024x768
System User
Username [wireless]
Full Name [Wireless Pentester]
Password [assign one]
Sound Card [detected]
Additional CDs [none]
Finish Setup

Configure Digitizer Pen (Wacom)
#cp /etc/X11/xorg.conf /etc/X11/xorg.conf.bak
#vim /etc/X11/xorg.conf

Add too Section "ServerLayout"

```
InputDevice    "cursor" "SendCoreEvents"
InputDevice    "stylus" "SendCoreEvents"
```

Add the following code after the mouse identification section and before the monitor identification.

```
Section "InputDevice"
       Driver        "wacom"
       Identifier    "cursor"
       Option        "Device"        "/dev/ttyS0"
       Option        "Type"          "cursor"
       Option        "ForceDevice"   "ISDV4"
       Option        "Mode"          "Absolute"
       Option        "Button3"      "2"
       Option        "Button2"      "3"
       Option        "TPCButton"     "on"
 EndSection

 Section "InputDevice"
       Driver        "wacom"
       Identifier    "stylus"
       Option        "Device"        "/dev/ttyS0"
       Option        "Type"          "stylus"
       Option        "ForceDevice"   "ISDV4"
 EndSection
```

Also edit /etc/rc.d/rc.local and add the line below to configure the serial interface to the tablet.

```
/bin/setserial /dev/ttyS0 port 0x0238 irq 4 autoconfig
```

Note: I am not a serial device expert and I found other tutorials with different numbers. How I found out what to put here was I booted to Ubuntu 7.04 Feisty Fawn. This distribution detects the pen automatically and searching dmesg will show the settings you need. Just search for 16550A as this is what the device is recognized as. Write down the info and reboot back into Fedora.

Note: When the stylus goes out of range from the screen, the mouse cursor warps to the top-left corner. When the mouse comes back in range, the cursor should warp back to the right spot. This can be particularly annoying if the temporary jump causes focus and menus to change. This is a known bug in the wacom X driver.

For setting up the YUM software management utility see this site:
http://www.fedorafaq.org/fc4/#installsoftware

#su –
cd /etc
#mv -f yum.conf yum.conf.bak
#wget http://www.fedorafaq.org/fc4/samples/yum.conf
#rpm -Uvh http://www.fedorafaq.org/fc4/yum http://rpm.livna.org/livna-release-4.rpm

Misc Commands:

#yum list available
#yum install packagename
#yum check-update

#yum update packagename
#yum search <word>

Update the Tablet!
Note: update yum and python first or you will get errors
#yum update yum
#yum update python
#yum update
REBOOT!

Madwifi
Wirelessdefense.org build a laptop howto for Fedora Core 4 – use this tutorial to configure the laptop with proper wireless drivers
http://www.wirelessdefence.org/Contents/WirelessBuildHowto.html
NOTE: using CVS to download madwifi no longer works because the driver is now ng (next generation) and we want the "old" version. Subversion (svn) should have been installed and will be used instead of CVS to checkout the drivers.

```
#svn checkout http://svn.madwifi.org/branches/madwifi-old madwifi
```

Madwifi-ng
You can also checkout the latest madwifi drivers and they will compile and install on the tablet. They will not work with the Karma framework because a new command (wlanconfig) is used to get the card in monitor mode and Karma does not know about it.

```
#svn checkout http://svn.madwifi.org/branches/madwifi madwifi
```

Prism Chipset – hostap drivers
Download the latest drivers from http://hostap.epitest.fi/releases (current hostap-driver-0.4.9)
#tar zxvf hostap-driver-0.4.9.tar.gz
#cd hostap-driver-0.4.9
#

IPW2100 – Intel mini-PCI wireless
The tablet has and on board wireless card supported by linux with the help of proprietary firmware from intel. We will download the latest drivers from http://ipw2100.sourceforge.net compile and install them. Then we will use yum to install the firmware
`#yum install ipw2100-firmware`
The firmware is placed in `/lib/firmware`

You can configure kismet source in kismet.conf to use this device in wireless sniffing
`source=ipw2100,eth1,ipw2100source`

Karma
Wirelessdefense.org build a laptop – install Karma wireless client hacking framework

http://www.wirelessdefence.org/Contents/KARMAMain.htm

Kismet

www.wirelessdefence.org has excellent instructions for installing kismet as well as all the software that kismet needs to be used effectively (i.e. imagemagick, gpsmap) Below is a rundown of what can be found on their site.

Download the latest gpsmap (currently gps-2.34) from
http://developer.berlios.de/projects/showfiles.php?group_id=2116

Download the latest ImageMagick from www.imagemagick.org

> NOTE: ImageMagick installs the library files that gpsmap needs in /usr/local/lib. Fedora by default does not know to look in this directory. Edit `/etc/ld.so.conf` and add `/usr/local/lib` to the end of the file. Then run `#ldconfig`

Download the latest GMP software from www.swox.com/gmp (tested with gmp-4.2.1.tar.gz)

Unpack each of these tarballs and ./configure, make, make install

```
#cd /tools/wifi
#wget http://www.kismetwireless.net/code/kismet-2006-04-R1-tar.gz
#tar zxvf kismet-2006-04-R1-tar.gz
#cd kismet-2006-04-R1
#./configure
#make
#make install
```

> NOTE: before installing kismet you may want to look at the instructions from www.wirelessdefence.org/Contents/Kismet Wireless Mapping.htm for instructions on patching gpsmap to include mapping from google.
>
> ```
> #cd /tools/wifi/kismet-2006-04-R1
> #wget  http://parknation.com/gmap/files/gpsmap-gmap-0.1.tgz
> #tar zxvf gpsmap-gmap-0.1.tgz
> #patch –p0 < gpsmap-gmap-0.1/gpsmap-gmap-0.1.diff
> #./configure
> #make
> #make install
> ```

Gpsdrive

http://www.gpsdrive.de download the latest stable version (currently 2.09)
NOTE: older version of gcc required.

```
#./configure
#make
#make install
```

Gournal – tablet note taking application

```
#yum install perl-Gtk2 perl-Gtk2-GladeXML perl-Gnome2-Canvas perl-
Gnome2 libgnomeprintui22-devel
#perl –MCPAN –e 'install ExtUtils::Depends'
```

```
#perl –MCPAN –e 'install ExtUtils::PkgConfig'
#perl –MCPAN –e 'install Gnome2::Print'
#perl –MCPAN –e 'install XML::Mini::Document'
```

Xvkbd – onscreen keyboard

```
#yum install Xaw3d Xaw3-devel
```

http://homepage3.nifty.com/tsato/xvkbd/#download

untar the source

```
#xmkmf; make install install.man
```

Add xvkbd to the login screen

edit `/etc/X11/xdm/Xsetup_0` and add `/usr/X11R6/bin/xvkbd &` to the end of the file Also you will need to change the login from gdm to xdm. Gdm does not support the on-screen keyboard. Desktop->System Settings->Login Screen : General Tab and change Greeter-Local to Standard Greeter

All set! Log out and try it!

Aircrack-ng

Download the latest stable release of aircrack-ng from www.aircrack-ng.org to the /tools/wifi directory. Unpack the archive and run make, make install

```
#tar zxvf aircrack-ng*.tar.gz
#cd aircrack-ng*
#make
#make install
```