

Forum:[Hack Forums](#)

Thread: [Legion | Hardware Hacking via Serial -- Basics](#)

PinkPanther - October 29, 2013, 10:41 am

[img]http://i.minus.com/ieq6viOQ6szdE.gif[/img]

Wifi guys:

This is a tutorial I posted in the legion sub forum a while back, and I just got permission to re-post it. This is a good starting point for learning firmware hacking on your 3g or wifi devices.

Many consumer devices are far more capable than the limited feature set exposed by the manufacturer. To have complete (or near complete) control of a device a person must go beyond pretty interfaces all the way to the serial headers found on the motherboard.

The Goal:Near unlimited control of the device.

Requirements:A device with serial headers

A multimeter

Basic electrical knowledge

Some wire

Level shifter (in some cases)

Overview:Locate serial header

ID serial pins

Connect wires from serial pins to PC

Connect to serial console via putty

In this tutorial I will use a wireless access point. In this case, I don't have the password to change any settings, but connecting to the serial console should give me root.

Step 1: Locate the Serial Header

-
-

-

-

Step 2: ID the Serial Pins

This is where basic electrical know how comes into play. There are typically four pins on each serial connector. At a bare minimum, a person needs at least three pins to control the device. One is a ground (GND), one is to receive output (RX), and one is to send commands (TX).

Identify the TX and GND connection using a multimeter set to DC voltage. Touch the black lead to a known electrical ground (usually the metal case or a large metal contact). Touch the red lead to each of the four pins. If the multimeter reads 0 volts on one of the four pins then that pin is either TX or Ground--If it is ground, it will also have continuity to ground which can be tested on a separate multimeter mode. TX will not also have continuity to ground.

-

-

*Using a DVOM to measure voltage between large metal ground and serial pins.

The remaining two pins will be RX and the not usually needed vcc. VCC will have a constant voltage of around ~3.3 volts while RX will have a changing voltage (if it is sending things for a to receive) .

Step 3: Connect Wires from Serial Port to PC

Once pins are identified, it is time to connect them to a PC. I use a TIAO USB Multi Protocol Adapter. It has the advantage of a TTL voltage shifter so I don't fry my device with PC power, and a USB port built in so I don't have to custom wire any adapters.

-

-

-

-

Step 4: Connect to the Serial Console with Putty.

At this point everything is connected. Putty can be used with the serial setting to connect to our device via its serial headers. If gibberish appears on the screen, you should change the line speed (baud rate). Usually settings are no flow control, no parity, 1 stop bits, and 0 data bits. Line speed varies.

The following video shows the boot process as seen from the serial console, after which I'm dropped to a root shell. Although I had no password, I was able to make all configuration changes and read from the shadow file.

TheCyb3rAlpha - October 29, 2013, 10:53 am

Its just AWESOME bro...

i did not understood the electrical part coz m just a cs grad but still its just way too good.
+3 rep if i could bro :D :D

PinkPanther - October 29, 2013, 3:15 pm

(Oct 29, 2013 10:53 AM)zircanavo_abyss Wrote: [\[CITE\]](#) Its just AWESOME bro...

i did not understood the electrical part coz m just a cs grad but still its just way too good.

+3 rep if i could bro :D :D

I never made it to grad school, but I majored in CS too brother. ? ?

ciocan - October 29, 2013, 4:46 pm

Excellent man!

Here what i found by mistake. Is about programing RTL8187.

ftp://ftp.emacinc.com/Controllers/Wireless/WLU54G_/User_Manual.pdf

and the software can be found in

ftp://ftp.emacinc.com/Controllers/Wireless/WLU54G_/

I hope to be useful for you and do some experiments. ?

I will write more but my english is limited...

Goodies - February 28, 2014, 10:53 pm

I'll kick this thread up... I really loved this when it came out. I bought an 'arduino' for it actually..

What would this work on, exactly? I have an ancient Linksys I got at a garage sale and I m going to try this out...

My 'arduinio' is actually a beaglebone (RPI alternative) so I'm not 100% sure it'll b able to work :P

PinkPanther - February 28, 2014, 11:05 pm

I'm using the TIAO only for level shifting since the voltages are TTL.

<https://www.sparkfun.com/tutorials/215>

You just need some kind of interface whether homemade or on a chip.

Goodies - February 28, 2014, 11:09 pm

(Mar 1, 2014 12:05 AM)PinkPanther Wrote: [\[CITE\]](#) I'm using the TIAO only for level shifting since the voltages are TTL.

<https://www.sparkfun.com/tutorials/215>

You just need some kind of interface whether homemade or on a chip.

Thanks! This is obviously not my area of study but I'm very interested in it. Appreciate it!

PinkPanther - February 28, 2014, 11:11 pm

(Mar 1, 2014 12:09 AM)Goodies Wrote: [\[CITE\]](#) Thanks! This is obviously not my area of study but I'm very interested in it. Appreciate it!

I did see a guy I think on google hangouts rooting his phone straight from the board. They always seem to leave the backdoor open for anyone who knows where it is.

PoLoW - March 2, 2014, 2:02 pm

Thanks for sharing OP you're such a HQ member .

Is it possible to Get a serial connection to Routers without USB ports ?

Clear Spot Voyager is what I'm aiming for , can we use this method to Get Root access ?

Keep up the Good work .

PinkPanther - March 2, 2014, 2:22 pm

(Mar 2, 2014 03:02 PM)PoLoW Wrote: [\[CITE\]](#) Thanks for sharing OP you're such a HQ member .

Is it possible to Get a serial connection to Routers without USB ports ?

Clear Spot Voyager is what I'm aiming for , can we use this method to Get Root access ?

Keep up the Good work .

You can do it without USB. There are several products that can do it or you can build your own.

tangoTT - March 2, 2014, 8:10 pm

(Oct 29, 2013 03:15 PM)PinkPanther Wrote: [\[CITE\]](#) I never made it to grad school, but I majored in CS too brother. ? ?

i have this calculator

[img]http://images04.olx-st.com/ui/8/44/45/1391357909_596873945_1-Pictures-of--Texas-Instruments-Nspire-CX-CAS-Graphing-Calculator.jpg[/img]

this is very interesting piece of hardware.

Can this calculator be hacked to load inside an linux or symbian os ???

?

h4x0rm1k3 - November 2, 2015, 1:33 am

I'm not 100% sure if this is what you mean but you can jailbreak the Nspire CX and run Android, Linux, Debian, Gameboy B&W and also colour as well as play Doom in B&W and colour! If you want a little more info about it then check out here -

<https://hackaday.com/tag/ti-nspire/>

Also here you'll find info on Doom & other TI hacks -

https://tiplanet.org/forum/archives_voir.php?id=3889

(Mar 2, 2014 09:10 PM)tangoTT Wrote: [\[CITE\]](#) i have this calculator

[img]http://images04.olx-st.com/ui/8/44/45/1391357909_596873945_1-Pictures-of--Texas-Instruments-Nspire-CX-CAS-Graphing-Calculator.jpg[/img]

this is very interesting piece of hardware.

Can this calculator be hacked to load inside an linux or symbian os ???

?

Siktah - November 3, 2015, 2:06 am

I know its an old thread revived but any idea on what to do when presented with a login over serial and no admin accounts are allowed to login?

h4x0rm1k3 - November 3, 2015, 6:43 am

I apologise for bringing up an old thread! For some reason it was on the 1st or 2nd page of the wifi section so I replied without noticing!

CraigghovenFN - October 9, 2026, 9:19 pm

This is exactly what i am trying to do with my embroidery machine, i have a machine that im trying to read data and create a remote connection to my mac and be able to log everything job i have.

i revealed the computer board and the manufacturer doesnt even have any sort of user manual (damn china) instructions