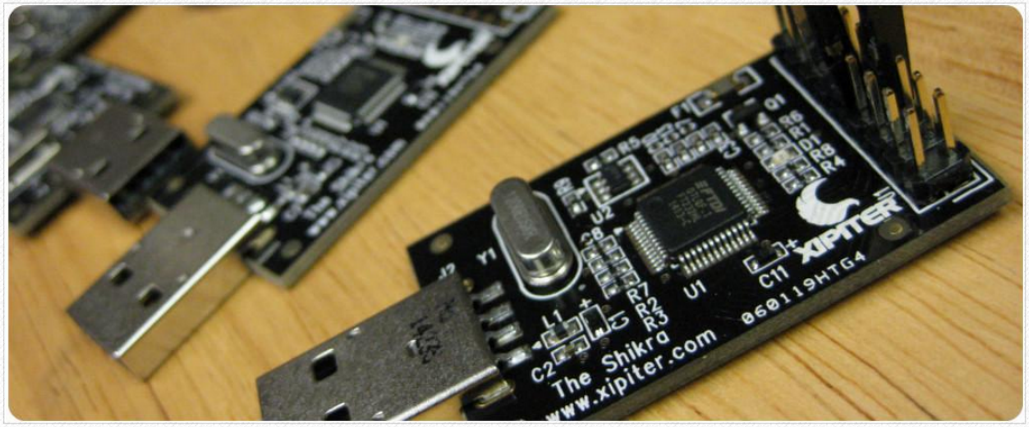
USING THE SHIKRA TO ATTACK EMBEDDED SYSTEMS: GETTING STARTED

12/26/2014 /

WHY "THE SHIKRA"?

Since we've started teaching SexViaHex, many people (not just our students) have asked me (Joe Fitzpatrick) for equipment recommendations for doing their own hardware hacking. I own and use several tools with duplicate and overlapping purposes, since there's usually a 'best' tool for any given job. In the process of assembling the equipment and content forSexViaHex, I had a hard time whittling it down. The first answer to 'what should I buy first?' is and will likely continue to be the BusPirate (with a Saleae in close second). No single tool speaks so many protocols, and only a handful of tools provide lots of the diagnostic and passive sniffing features of the BusPirate.



Purchase a Shikra here at INT3.CC

Once you've identified all your pin-outs, protocols, data rates, and device addresses, It's usually best to move on to more robust single-purpose tools. (Techniques and tricks for doing this we focus on quite a bit in our SexViaHex course.). We had a hard time choosing which tools to include in the class since there are so many choices and limited time in our class, and limited space in our Student Kits.

FTDI's FT232H chip is the more powerful older brother to FT232R USB to UART adapter. The "-H" model of chips are widely used in JTAG adapters but also support several different serial protocols, plus the ability to bit-bang custom ones. The Shikra is Xipiter's nice, dead-simple FT232H device that allows you to use all these different modes. *(FYI: Keeping with the "accipiter" theme at Xipiter, Shikra was also named after a bird of prey.)*

So what practical things can you do with it? Here's a few things I've done with it so far.

THE SHIKRA FOR UART:

The bus pirate has several UART features like passive sniffing, baud detection, and a transparent passthrough mode. It should let

OTHER NEWS

Read Xipiter Newsletters

RSS Feed

UPCOMING TRAINING

Practical Android Exploitation

Blackhat, Las Vegas 2018
SOLD OUT

2019 - TBA

Software Exploitation Via Hardware Exploitation

Blackhat, Las Vegas 2018
SOLD OUT

2019 - TBA

Practical ARM Exploitation

2019 - TBA

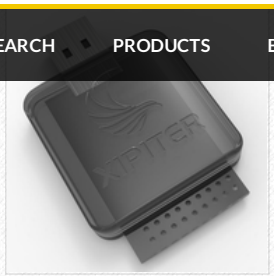
HackAWebcam Workshop

2019 - TBA

BLOG CATEGORIES

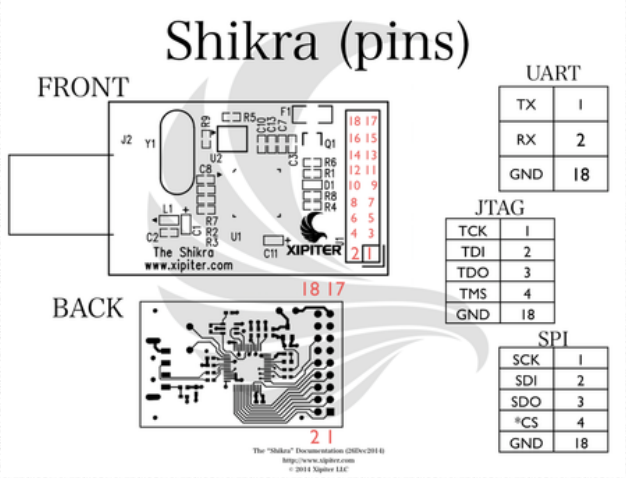
All
Embedded Devices
Exploitation
INT.CC
Iot
Research
The Insecurity Of Things

you do most of what you need to over UART. Usually once i've figured out my pinout and baud rate, i switch to a simple USB TTL Serial cable to free up my bus pirate for better things. On the access-point/router shown below, UBOOT runs at 120kbps while the kernel (which loads after) boots at slower 115.2. The bus pirate tends to be very picky and fails if the baud rate is only slightly off, while a dedicated cable usually has a wider tolerance and can read both with no settings change. The Shikra had no problem with this.



The Shikra case.

"So hold on a second" (you might be thinking) "First things first! How to we wire this Shikra up to stuff?" It's really simple, the Shikra much like the BusPirate just has headers which you can use to jumper to your target. The pinouts of the Shikra are viewable in the documentation for it.



Pinouts for the Shikra (the "back" is mirrored)

According to the diagram to the above, UART, the Shikra's pinouts are as follows:

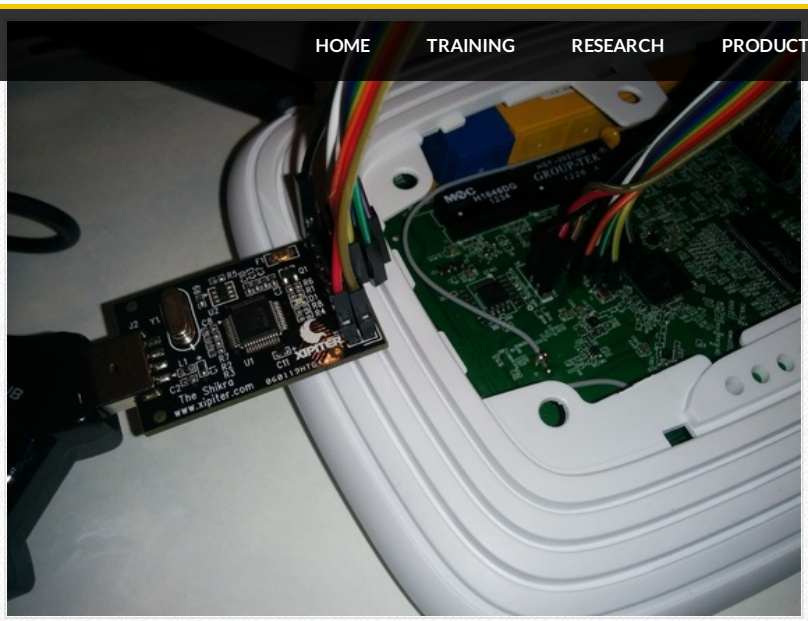
TX: 1
RX: 2
GND: 18

Once wired up, the following command (from a *nix) machine will connect you through the Shikra to whatever you're targeting:

$ screen /dev/ttyUSB0 115200

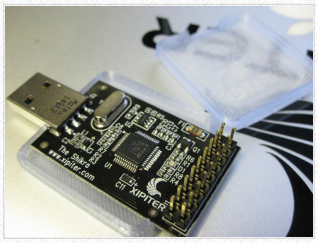
***Protip**: I never worry about getting TX and RX right, since somewhere along the way they get mixed up, and it's usually easier to swap them once to get things to work than it is to make sure they're right in the first place.*

ELSEWHERE...



The Shikra acting as UART adapter to attack a router/access point.

THE SHIKRA FOR JTAG:



The Shikra in a 3D printed version of its case .

JTAG adapters run $10 to $20,000 - but in the end they're all speaking the same protocol. For SexViaHex, we needed to use JTAG at the same time as UART so we knew we needed a second device. We tried using EZ-USB FX2 boards, but had trouble reliably sourcing them. The first time we taught the class, we used the Bus Pirate since it is well supported by OpenOCD - however it's **incredibly** slow, and required frequent reconnecting for hardware reset.

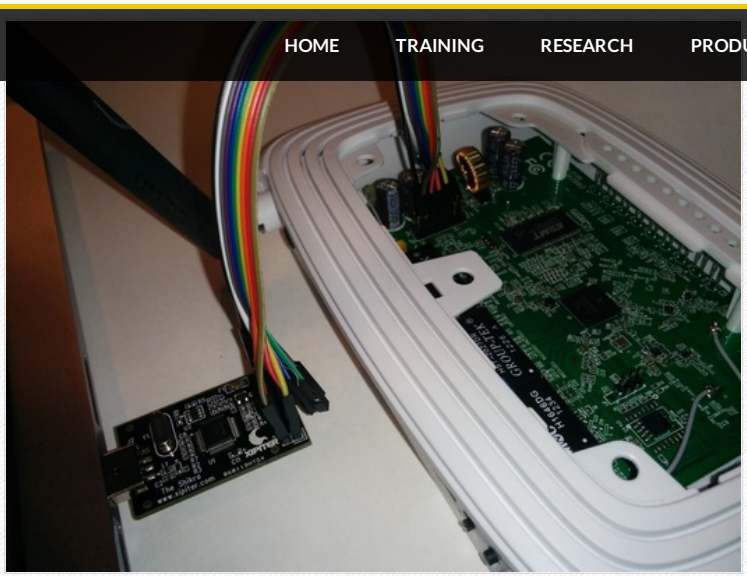
We needed something different so we switched to a different FT232H-based board that worked well, but has had a very high failure rate (they'd burn up easily or stop working inexplicably). We needed something more reliable. So after all that we decided to design something and the Shikra eventually replaced these tools. The Shikra was equally as easy to get wired up for JTAG and use with OpenOCD:

Shikra JTAG Pinout:
TCK: 1
TDI: 2
TDO: 3
TMS: 4
GND: 18

OpenOCD Config File for the Shikra:

```
#shikra.cfg
interface ftdi
ftdi_vid_pid 0x0403 0x6014

ftdi_layout_init 0x0c08 0x0f1b
adapter_khz 2000
#end shikra.cfg
```



The Shikra as a JTAG adapter to attack a router/access point.

I've also been looking for a reliable JTAG adapter for FPGA configuration for the WTFPGA workshop I've been doing at some conferences. Thanks to some open source developers, there's an alternative to the pricey Xilinx Platform Cables that works with the native configuration tool. I followed the same process that Colin O'Flynn did for the older FT2232D:

THE SHIKRA FOR SPI:

Embedded devices can add a few bytes to a few megabytes of storage for under a dollar with a tiny 8-pin SPI flash chip. There are also SPI network adapters, A/D converters, and all sorts of other devices, but the firmware on SPI flash chips is usually what's most interesting.*(For more interesting devices that SPI can be found in, see the Xipiter talk "Hardware Hacking for Software People").*

> **Where the BusPirate took ~30 minutes to extract a 4MB firmware image from a device, the Shikra took less than a minute!**

A DediProg SF-100 Flash Programmer in the Xipiter lab.

One exercise we have in SexViaHex is to pull off the full firmware image from an embedded device. We use a clip like a Pomona 5250to directly contact the 8-pin SOIC chip's pins without having to desolder, and then we use the bus pirate and Flashrom to 'quickly' dump a 4MB firmware in 20 minutes - if it works the first time. Specialized devices like a Dediprog SF100 (pictured to the left) would be much quicker, but are a bit to large and expensive for us to buy 30 to put into our student kits for SexViaHex. Luckily Shikra supports SPI, and flashrom supports a generic FT2232 interface, allowing firmware dumps in less than a minute.

Shikra SPI Pinout:
SCK -1
SDI - 2
SDO -3
*CS - 4
GND - 18

To dump an SPI flash with the Shikra we simply:
$ flashrom -p ft2232_spi:type=232H -r spidump.bin

The Shikra "un-bricking" a tablet by overwriting firmware via SPI using a 8-pin SOIC clip. The SOIC clip made this "unobtrusive" not requiring the chip to be desoldered!

Of course, Shikra is not just for work. I recently got a Teclast Air II tablet (same panel as an ipad retina, but with an intel bay trail SOC and andriod/win8). I wanted to update it to a dual-boot bios, but accidentally bricked it because i flashed a bios file for the older Teclast Air 3G. Luckily i was able to resurrect it by using the Shikra + Pomona SOIC + Flashrom to directly flash the chip when it wouldn't boot otherwise.

In summary, I was pretty excited to get my hands on Shikra, and I'm looking forward to showing participants in our future SexViaHex classes how to use it to reverse engineer and hack up hardware devices!

YOU CAN PURCHASE A SHIKRA HERE!

shikra_documentation.pdf
Download File

DOWNLOAD A PDF OF THE SHIKRA PINOUTS TO THE LEFT!

Comments are closed.

toll-free: 1.855.XIP.ITER main: 1.646.783.3999 fax: 1.917.746.9832 email: info (@) xipiter (dot.) com