EXPLIOT
www.expliot.io

Introduction To Hardware

UART

Introduction to UART

IoT Hardware Attack Surfaces

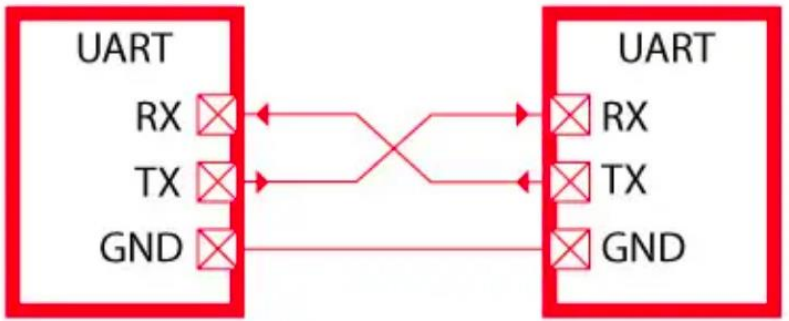
- Hardware Debug ports
  - UART
  - I2C
  - SPI
  - JTAG
  - SWD

Introduction

- Universal Asynchronous Receiver and Transmitter
- UART Protocols is a serial communication with two wire protocol.
- The data cable signal lines are labelled as Rx and Tx.
- Simple way to transfer data directly to and from microcontrollers without the need of any intermediary hardware
- No ACK protocol
- Most commonly used in embedded devices

Introduction

- Transmitting UART converts parallel data into serial and transmits
- Receiving UART converts received serial data into parallel
- Data flows from the Tx pin of the transmitting UART to the Rx pin of the receiving UART

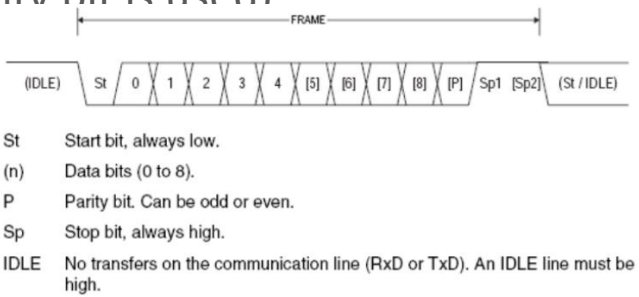


Source: https://microcontrollerslab.com/uart-communication-working-applications/

Introduction

- It has one start bit, 5 to 8-bit data and one stop bit mean the 8-bit data transfer ones signal is high to low.

- Start Bit – Low / Space / 0 / Positive voltage
- Stop Bit – High / Mark / 1 / Negative voltage
- Parity Bit – Optional, used if no. of bits per character are not 9
- Data bits – 5-8 (or even 9, in which case no parity bit is used)
    - Least significant bit sent first



Source:
http://web.engr.oregonstate.edu/~traylor/ece473/lectures/uart.pdf

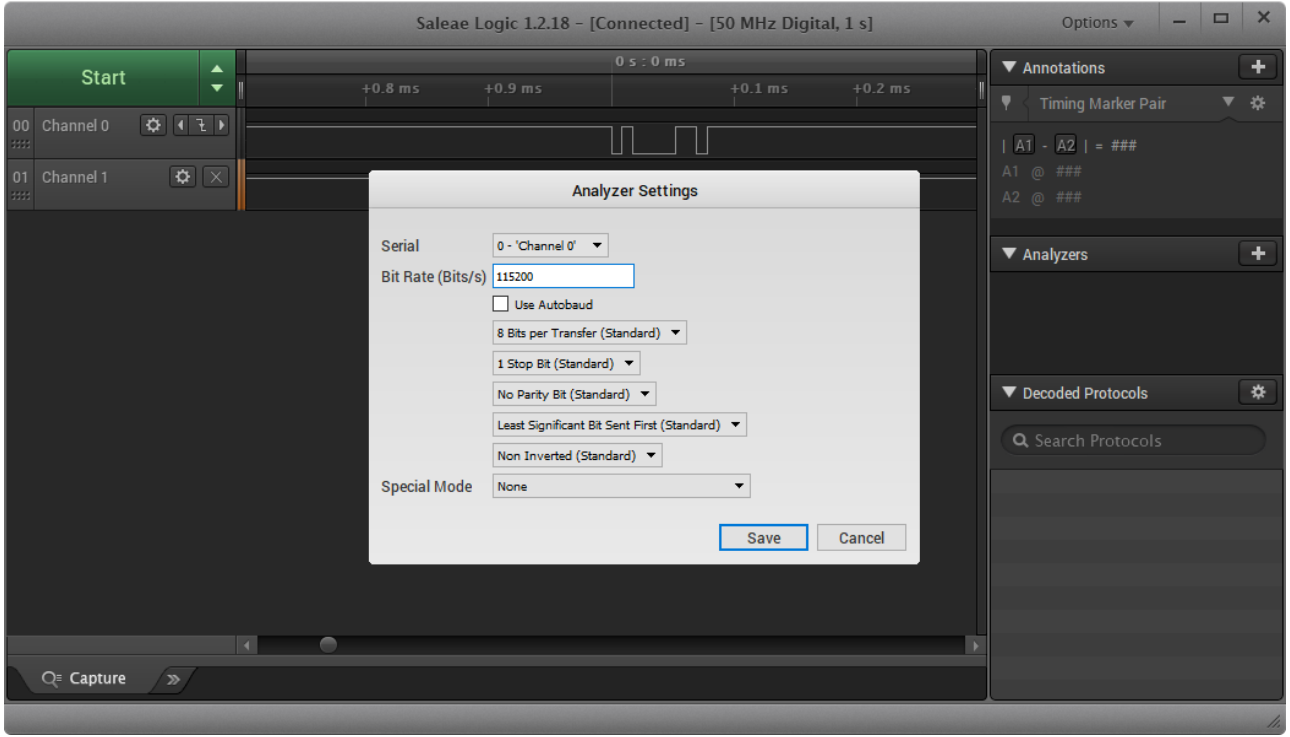
Baudrate

- Oversample rate
  - 4,8,16,32
- Peripheral clock
- Baud rate divider
- Standard baudrates like 9600,38400,115200

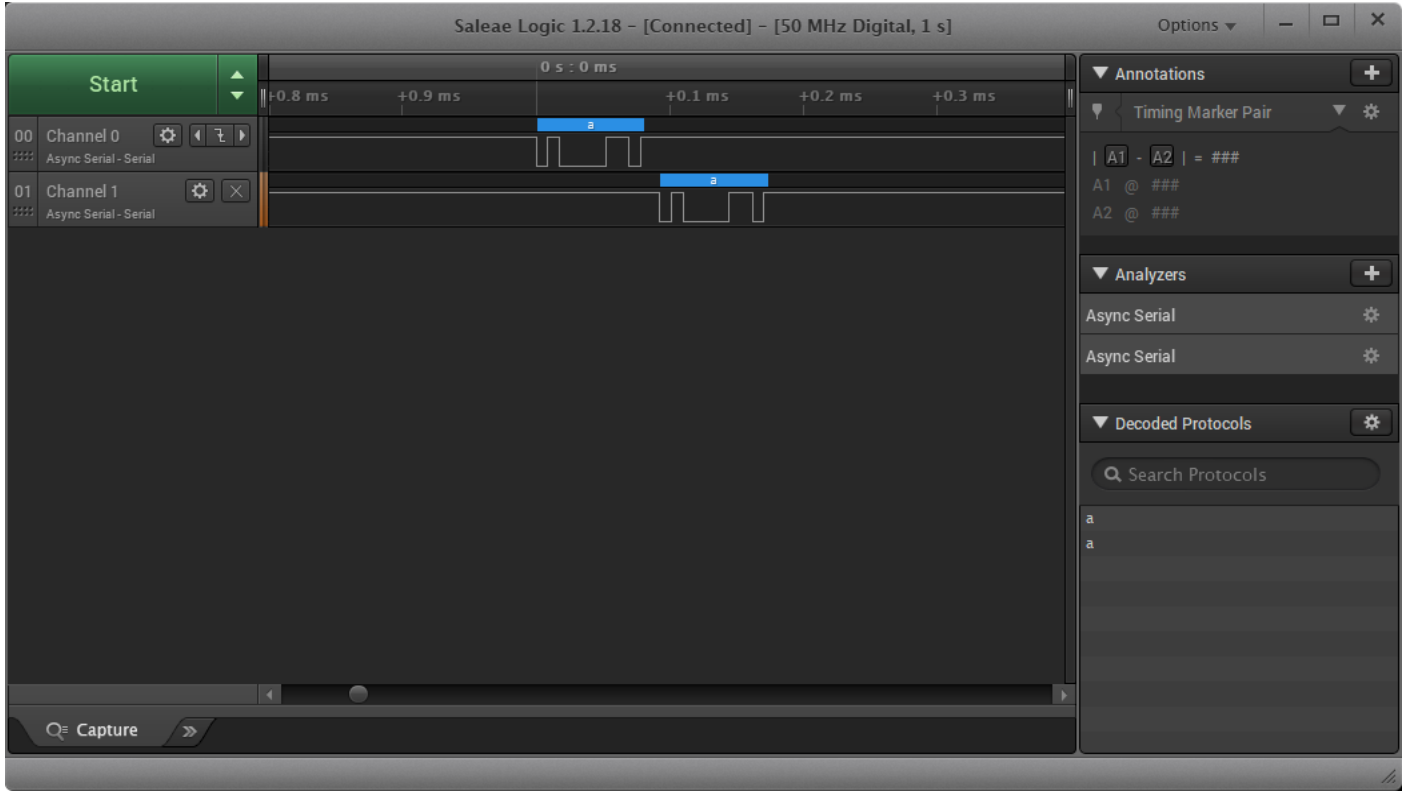
Possible Attacks

- Get root shell
- Sniff communication
- Signal tampering

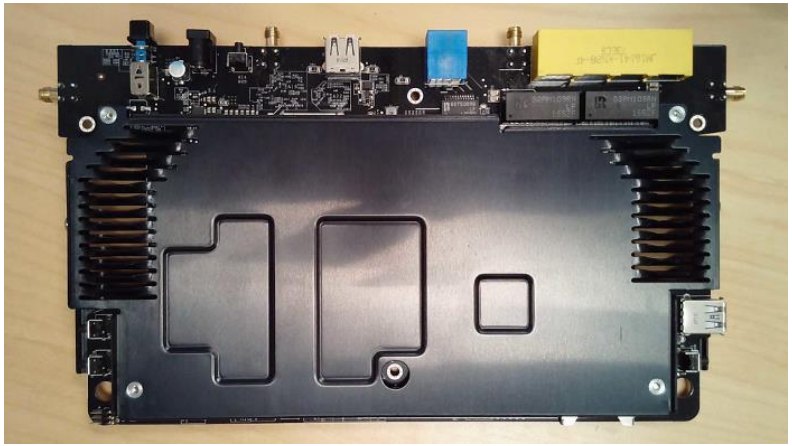
UART Sniffing



UART Sniffing

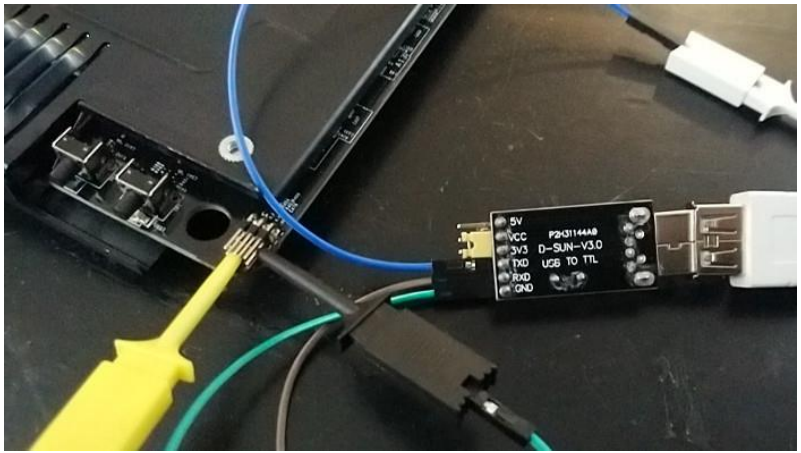


UART Shell



Source:
https://www.ethicalhacker.net/columns/sindermann/hardware-hacking-101-lesson-3-abusing-uart-u-are-root/

UART Shell




```
[   68.682380] [wifi0] FWLOG: [69614] VDEV_MGR_HP_START_TIME ( 0x0, 0x1685, 0x246d001 )
[   68.689940] [wifi0] FWLOG: [69614] RESMGR_OCS_GEN_PERIODIC_NOA ( 0x1 )
[   68.696438] [wifi0] FWLOG: [69614] RESMGR_OCS_GEN_PERIODIC_NOA ( 0x0 )
[   68.702936] [wifi0] FWLOG: [69614] VDEV_MGR_AP_TBTT_CONFIG ( 0x0, 0x1685, 0x0, 0x0 )
[   69.721680] Enabling NSS RPS
[   70.150859] EXT4-fs (mmcblk0p6): barriers disabled
[   70.156982] EXT4-fs (mmcblk0p6): mounted filesystem with writeback data mode. Opts: data=writeback,ol
dalloc
[   70.621868] Adding 262140k swap on /volume1/.intswp.  Priority:999 extents:2 across:270332k SS
[   70.742674] synoiprecord: Init successfully
[   71.497625] [SYNO] success to create syno_netlink_sock(28)
[   72.017744] usbcore: registered new interface driver usblp
[   72.241830] eth2: 10 Mbps Half Duplex
[   73.276288] ADDRCONF(NETDEV_CHANGE): eth2: link becomes ready
[   73.283036] lbr0: port 2(eth2) entered forwarding state
[   73.287285] lbr0: port 2(eth2) entered forwarding state
[   73.720587] __mc_netlink_receive: Disable bridge snooping!

SynologyRouter login: [   74.279100] lbr0: port 2(eth2) entered forwarding state
[   76.487097] init: httpd-sys main process (14279) killed by TERM signal
[   78.904873] loop: module loaded
[   84.371009] findhostd uses obsolete (PF_INET,SOCK_PACKET)
[   86.432052] [SYNO] release syno_netlink_ctf_sock(d381ba00)

SynologyRouter login:
SynologyRouter login:
SynologyRouter login:
```

Source:
https://www.ethicalhacker.net/columns/sindermann/hardware-hacking-101-lesson-3-abusing-uart-u-are-root/

UART Interfacing

Challenges in Accessing Unknown UART

- Pin identification
- Baudrate

UART identification

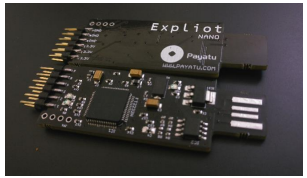
- First step in accessing the device is to identify the UART interface
- UART usually has 4 pins
  - GND – Ground
  - Rx – Receive
  - Tx – Transmit
  - Vcc – Voltage
- If we find a set of 4 pins together, we can hope it’s a UART port

UART identification

- Manual Identification methods
- Method 1 - Digital Multimeter Conductivity Test
- Method 2 - Analyzing PIN voltage and conductivity
- Automated Identification methods
- Using in EXPLIoT Bus Auditor and EXPLIoT Nano

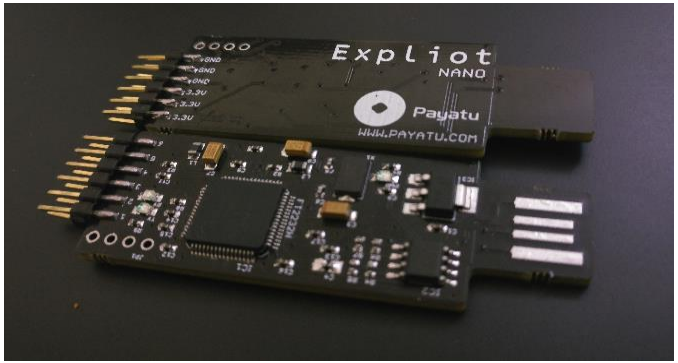
UART: Things you need

- Device
- Multimeter
- Expliot Nano and cables
- Wires
- Terminal Emulator (minicom etc)
- Pair of eyes
- Phone flashlight just in case
- Soldering kit if the wires need to be soldered to the pins



EXPLIoT Nano

- Expliot-NANO is a compact hacker friendly multi-purpose, multi-protocol hardware tool mainly used to debug and program microcontrollers/processors and flash chips
- Expliot-NANO can be configured to support hardware protocols including, UART, I2C, SPI, ARM SWD and JTAG.

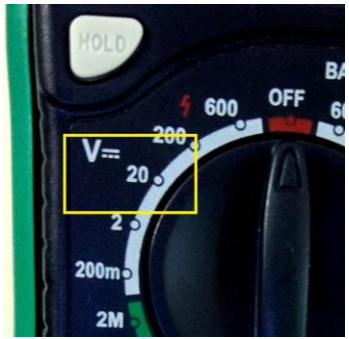


EXPLIoT Bus Auditor

- BUS Auditor is a compact multi-protocol tool used for scanning and identifying debugging and communication interfaces exposed on any hardware board
- It can brute force several hardware protocols including JTAG, arm SWD, UART, and I2C.
- The device has 16 channels, every channel can be used to interface with a pin-out on the target board.

Manual Method for UART Access

- UART pin and Baudrate identification
  - Identify ground pin and Vcc with multimeter
  - Connect the remaining 2 pins as Tx or Rx to UART converter
  - Refer the data sheet of the MCU if needed
  - Try standard baurates while you get acess
- Problem
  - For bigger products with multiple UARTs this is tedious and boring process
  - Needs lot of tracking of pins



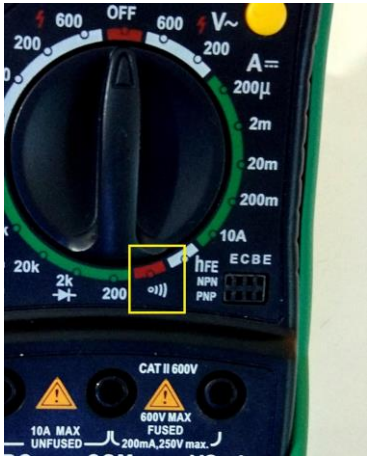
Identify

- Test each pin with multimeter to identify its purpose
- Start with GND
- Vcc
- Tx
- Rx

Identify GND

- Make sure device is powered off
- GND may also look like this -->
- Multimeter continuity test

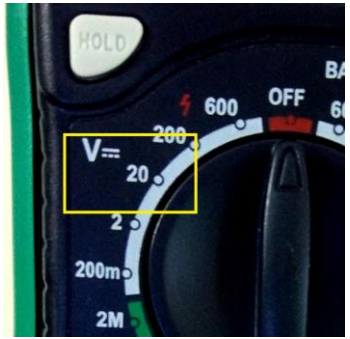
- Point the rotary switch to continuity test
  - the option that looks like this -> o)))
- Identify any metallic sheet area
- Put the red probe on the pin to be tested
- Put the black probe to the GND of input supply
- If the multimeter makes continuous beep it is a GND pin



Identify Vcc

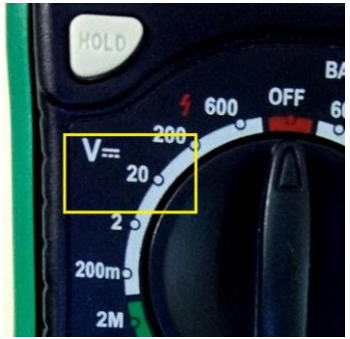
- NOTE: Vcc is not used when connecting to serial interface, but identifying it helps in narrowing our search for Tx and Rx
- Power on the device
- Multimeter Voltage test

- Point the rotary switch to V (20)
  - (assuming voltage under 20)
  - Incidentally the rotary switch is pointing to V 20 in the image :)
  - Put the red probe on the pin to be tested
  - Put the black probe on the identified GND pin or GND of input supply
  - If the multimeter displays fairly constant voltage (for ex. 3.3) it is Vcc



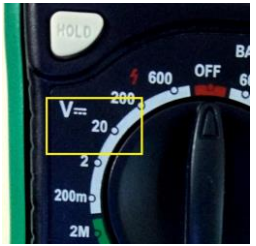
Identify Tx

- Power on the device and immediately do the multi-meter test
- Multimeter Voltage test
- Point the rotary switch to V (20)
  - Assuming voltage under 20
  - Incidentally the rotary switch is pointing to V 20 in the image :)
- Put the red probe on the pin to be tested
- Put the black probe on the metallic area
- If the multimeter displays varying voltage it is likely a Tx pin
- If not, Repeat with other pins till you find one



Identify Rx

- Little difficult to identify Rx as there are no specific traits
- Power on the device and immediately do the multimeter test
- Multimeter Voltage test
- Point the rotary switch to V (20)
    - Assuming voltage under 20
    - Incidentally, the rotary switch is pointing to V 20 in the image :)
- Put the red probe on the pin to be tested
- Put the black probe on the metallic area



Identify Rx

- Multimeter Voltage test
- Put the black probe on the metallic area
- In some cases will show constant voltage either low or high
- In some cases it will show varying voltage
- In my experience I have encountered constant low voltage
- If not found, Repeat with other pins, if any left, till you find one

NOTE: If we identify the other 3 pins successfully, and there are only 4 pins then the one left is Rx

Identify Rx

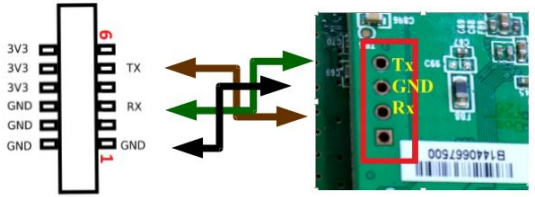
- Multimeter Voltage test

- Put the black probe on the metallic area
- In some cases will show constant voltage either low or high
- In some cases it will show varying voltage
- In my experience I have encountered constant low voltage
- If not found, Repeat with other pins, if any left, till you find one

NOTE: If we identify the other 3 pins successfully, and there are only 4 pins then the one left is Rx

Interface

- Connect the Expliot Nano with the UART pins on the board using wires and breakaway headers.
- Check Expliot Nano Specs for pin details
- Solder wires/headers if required



Expliot Nano TX <---------- > RX UART Pin on board

Expliot Nano RX <---------- >TX UART Pin on board

Expliot Nano GND <----------> GND UART Pin on board

Access

- The port can be accessed via /dev/ttyUSB0
- Power on the device and immediately run a serial console utility
- Utilities for serial console access
  - Minicom/picocom
  - Screen
- Cmd: sudo minicom -b <baudrate> -D <device>

  -b <baudrate>: baudrate to use, default is 115200

  -D <device>: serial port to use for ex. /dev/ttyUSB0

  Ex: sudo minicom -b 115200 -D /dev/ttyUSB0

Access

- Most devices will have default baudrate of 115200
- If you see binary garbage data it is most likely that the baudrate specified is wrong.
- Use Baudrate.py – An excellent tool to detect baudrate created by Craig Heffner
- Source: https://code.google.com/p/baudrate/
- Next slide shows how to use baudrate.py

Access

- Power on the machine and immediately run baudrate.py
- Cmd: sudo baudrate.py -p <serial port>
- Ex: baudrate.py -p /dev/ttyUSB0
- Down arrow key will cause baudrate.py to shift to a lower baudrate
- Up arrow key will cause baudrate.py to shift to a higher baudrate
- It starts with 115200. if you see garbage press down arrow and test with lower baudrate, repeat it till you find the correct baudrate
- Baudrate.py -a option auto detect mode, so you dont have to press Up/Down arrow keys

Access

- Once it is detected Press CTL-C and baudrate will ask you for a name to save the config for minicom (give any name, you can later run sudo minicom <name> to use the correct configuration)
- It will also ask you if you want to run minicom, choose yes and run it.
- NOTE: You may not get shell in baudrate.py, so you may have to let baudrate.py run minicom(CTL-C in baudrate.py as mentioned above), once minicom runs, press enter to check the shell
- To exit from a minicom session Press CTL-A and then X

Automatic Method for UART Access

- UART pin and Baudrate identification
  - Identify ground pin
  - Connect the debug port pins on device to bus auditor
  - Scan for the pins in EXPLIoT framework
  - Bus auditor will provide Tx and Rx pins with the baudrate
- UART Shell Access
  - Connect the identified Tx, Rx and Gnd pins to Rx, Tx and Gnd pins of EXPLIoT nano

Demo

The End