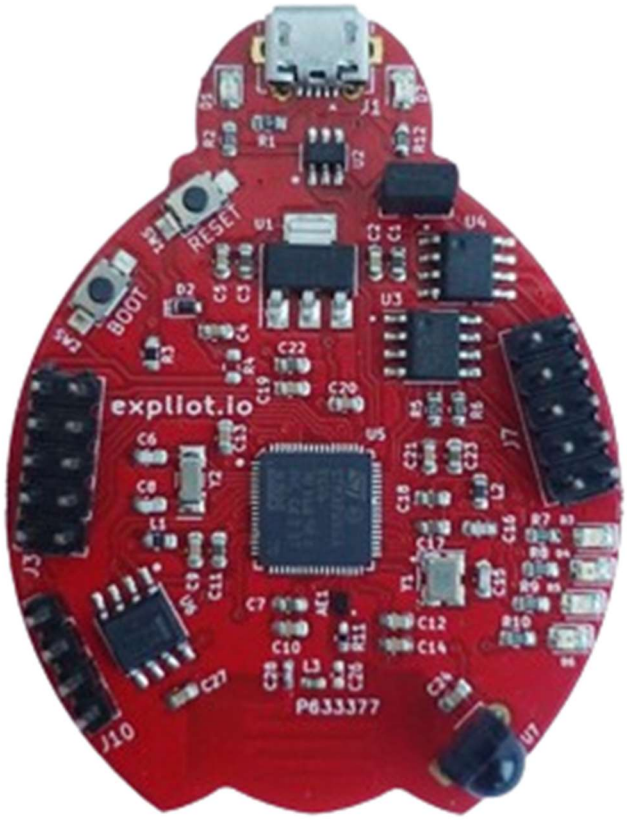
DAMN INSECURE VULNERABLE APPLICATION BOARD

Connected IoT device and vulnerable target board



Welcome to DIVA

Quick Start Guide

Damn Insecure and Vulnerable Application board is a connected IoT device and a vulnerable target board designed to teach the basics of IoT security.

DIVA integrates multiprotocol wireless 32-bit MCU Arm-based Cortex M4, Bluetooth and 802.15.4 radio solutions on the board. It comes with many more on-board peripherals including, SPI and I2C EEPROMS, IR receiver, temperature sensor etc.

The board provides a standard JTAG debug interface as well as an SWD port that can be used to debug programs from the host PC. The inbuilt USB port can be used for accessing the serial console and for firmware upgrades in DFU mode.

Features

1. USB 2.0 virtual com interface
2. USB Device Firmware Upgrade (DFU) support
3. Memory - onboard 256 kb I2C EEPROM and 256 kb SPI EEPROM Standard JTAG debug interface as well as ARM SWD interface.
4. GDB Debugging support - Can be used with any openOCD supported debugger/programmer.
5. UART debugging port.
6. Exposed I2C and SPI lines for ease.
7. Access to Built-in ZigBee/802.15.4 radio.
8. Access to Built-in BLE 4.0.

System requirements

PC with at least one USB port

Power input: 5V through the USBport

Operating system: Linux, Windows, MAC.

Dimensions

LxW: 57 mm x 45mm.

Weight: 15 gms

Getting started with your DIVA board

1. Connect DIVA board to PC using the given micro USB cable. Make sure that jumper J2 should be present on board. Please refer above image for reference.
2. You need to have a serial terminal application installed on the PC. Please install it if you don't have one.
   Serial terminal applications: **screen** (Linux, Mac), **teraterm,**
   putty(Windows)
   https://linux.die.net/man/1/screen
   https://osdn.net/projects/ttssh2/releases
3. The open screen in the terminal passing path to the connected DIVA. (In windows open teraterm and configure the corresponding COMport)
   sudo screen <path_to_the_tty>
   eg: sudo screen/dev/ttyACM0
   Please note: baud rate is not required.
   You may choose a baud rate of 9600 if thedevice is not working with the default baud rate.
   You will get DIVA console, through which we can navigate to the challenges
4. In the console type **.h** and Enter for help and type **.l** (dot el) to Enter for listing of LABS. You may choose a LAB from the list

PRE-FLASHED LABS:

I2C sniffing Lab:

The objective is to sniff the I2C communication (between the microcontroller and I2C EEPROM) using a logic analyzer to break the authentication mechanism.

UART port Lab:

The objective is to identify the UART port, performing a conductivity test between microcontroller pins and pin headers on the board using a digital multimeter. Once identified the port, you can connect a USB-TTL or EXPLIoT Nano to it.

SPI sniffing Lab:

Objective is to use a logic analyzer to sniff the microcontroller-SPI EEPROM communication and to break the authentication mechanism.

ZigBee Lab:

Students can eavesdrop the IEEE 15.4 communication and learn to replay it.

BLE Lab:

Like Zigbee Lab, students or learners can learn the BLE 4.0 communications eavesdrop and replay.

Firmware analysis Lab:

Objective is to break device authentication, by modifying the hardcoded password in the firmware. Firmware can be extracted and written back over JTAG interface. To identify the JTAG port you can perform conductivity test or brute-forcing using JTAGulator/JTAGenum.

Hidden command Lab:

There is a hidden command in the console, objective is to identify this backdoor. You may use a scripting language to automate the process.

Flashing firmware:

All the boards we sent out are tested and flashed with the latest firmware, still you mayneed to re-flash the firmware,

we will provide the firmware in case If the current firmware not working properly.

Currently, we only support flashing from a Linux PC. You need to have **dfu-utils** installed on the PC

1. Connect DIVA board to the PC through a micro USB cable.
2. To put the device into Device Firmware Upgrade (DFU)mode,
   Press and hold the **BOOT** button, then press and release the **RESET** button,
   after a few seconds release the **BOOT** button.
   You can verify DFU mode using **lsusb** command in the terminal.
3. Flashing firmware using **dfu-utils:**

   dfu-util -a 0 -s 0x08000000:leave -D <path_to_the_upgrade_file>

   Run above command, replace**<path_to_the_upgrade_file>**with the actual firmware path, where you have stored the .bin file of DIVA F/W.