Tigard Applied Physical Attacks Online Kit
TIGARD-KIT-V1
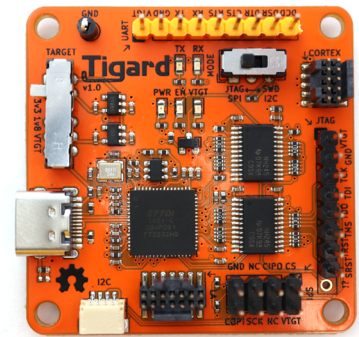
Product Overview
10-27-2022
For the most up-to-date information, visit www.mouser.com or the supplier's website.

Description

Crowd Supply Tigard Applied Physical Attacks Online Kit creates the tool needed to teach hardware hacking basics on embedded and IoT systems. This kit includes Tigard, BitMagic basic, wires, harnesses, clips, connectors, and a USB microscope. The Tigard applied physical attacks online kit also includes a simple multimeter and an organizer pouch.

The Tigard applied physical attacks online kit goes hand-in-hand with online access to 3+ days of lectures, labs, and support that helps identify and connect to undocumented interfaces, dumping, analyzing, emulating, and modifying firmware in multiple ways.

The Tigard combines support for all of the most-used interfaces and most-needed features onto a simple board. This device features a USB Type C high-speed (480Mbps) interface, a Logic Analyzer (LA) port to observe device-level signals, and a switch to choose between SPI/JTAG and I²C/SWD modes.

Features

- USB Type C high-speed (480Mbps) interface
- FTDI FT2232HQ dual high-speed USB to multipurpose UART/FIFO IC:
  - Primary port dedicated to UART, including access to all flow control signals
  - Secondary port shared among dedicated headers for SWD, JTAG, SPI, and I²C
- High-performance directional level-shifters for 1.8V to 5.5V operation
- Switch to choose between on-board 1.8V, 3.3V, 5V, and off-board vTarget supplies
- Switch to choose between SPI/JTAG and I²C/SWD modes
- Logic Analyzer port to observe device-level signals
- Indicator lights to aid in debugging

Kit Contents

- Tigard
- BitMagic basic
- Wires, harnesses, clips, and connectors
- A simple multimeter
- An organizer pouch
- A USB microscope
- A prepared target system:
  - Linux-based Wi-Fi router

Mouser Part Number

[View Part](#)

To learn more, visit
https://www.mouser.com/new/crowd-supply/crowd-supply-tigard-app-physical-attacks-kit/