

### Join GitHub today

Dismiss

GitHub is home to over 36 million developers working together to host and review code, manage projects, and build software together.

Sign up

#### Tecktronx MSO20xx/DPO20xx software hack for AppModules

1 commit

1 branch

0 releases

1 contributor

Branch: master

New pull request

Find File

Clone or download

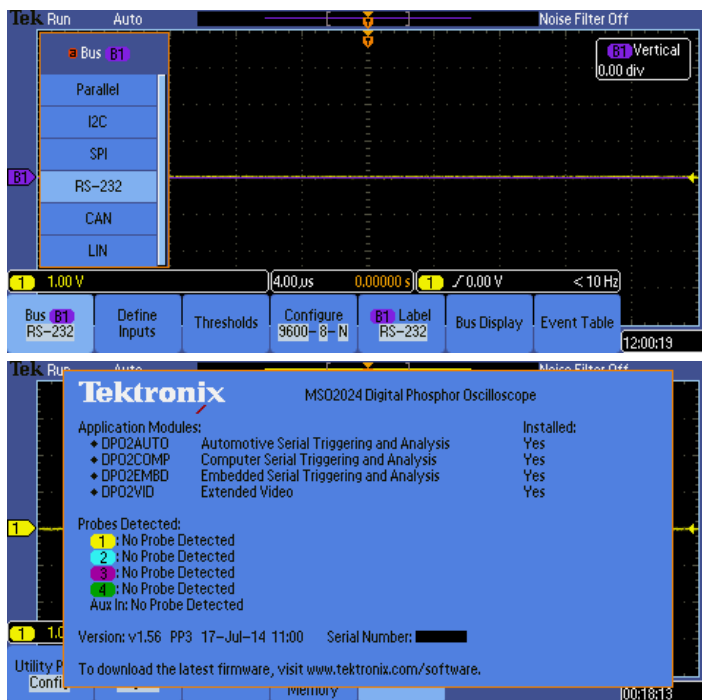
John Ripper	Initial commit	Latest commit 5807f72 on May 26, 2015
aux	Initial commit	4 years ago
src	Initial commit	4 years ago
tools	Initial commit	4 years ago
.gitignore	Initial commit	4 years ago
Makefile	Initial commit	4 years ago
Readme.md	Initial commit	4 years ago

Readme.md

# Tektronix MSO20xx/DPO20xx application module soft-emulator

## Background

The project aims to remove ridiculous restrictions on usage of AppModules in Tektronix oscilloscopes.



A well-known solution how to hack the appmodules can be found on [hackaday](#). However, it requires building a hardware module.

Another approach is demonstrated here: it uses `LD_PRELOAD` technique to override access of scope application to i2c bus and emulate AppModule keys. Investigation of `scopeApp.ppc8xx` revealed that in MSO20xx/DPO20xx it scans two addresses (namely, `0x50` and `0x52`) and tries to read 1 byte from those addresses. If succeeded, it changes base address to `0x4` (by writing `0x4` to the slave) and reads back 15 bytes. The `override.so` module simply gives the application what it's expecting to see.

Furthermore, a patch for binary file `scopeApp.ppc8xx` (`src/binpatch.sh`) is provided. It changes `fpAppKeyInitAdrrs` to look at addresses `0x50`, `0x51`, `0x52` and `0x53` thus giving ability to unlock 4 AppModule simultaneously.

## Prerequisites

- Cross-compiler for `ppc32`
- Swiss File Knife `sfk` (if you intend to apply binary patch on `scopeApp.ppc8xxx`)

I've used a VM with debian sarge to build cross-compiler using `crosstool` project (`powerpc-405`, `gcc-3.3.6`, `glibc-2.3.6` work fine for me).

## Build & Install

Assuming that you have cross-compiler for `powerpc32` and `sfk` in right paths (see Makefiles for that), you can just use `make` to build the firmware. Put it to your usb flash drive and follow usual Tektronix manual on updating the firmware.

## Dedications

This hack is dedicated entirely to greed of Tektronix sales managers (especially those in Russian Federation) who completely fail to publish GNU GPL software components used in their scopes (`linux kernel`, `glibc`, `busybox`).

## Legal notice

I assume that you do not use this to "crack" Tektronix scopes. Please feel free to unlock only features you have purchased from Tektronix. This software is intended to be used if you've lost the hardware key or it has been broken (or simply you don't like the idea of HW modules to unlock SW features).