

TEW-652BRP hacking

- Download GPL code from TrendNet:
 - <http://downloads.trendnet.com/gpl/>
 - Untar/unzip into /home/ directory
 - Read TEW-652BRP_BuildProcess.txt
 - Untar toolchain/ap71.tar.bz2 onto /opt/
 - cp
WWW/TEW-652BRP/config/TEW-652BRP.prj.config .config

TEW-652BRP hacking

- Build GPL firmware image
 - Run make menuconfig, edit the configuration
 - Run `make 2>&1 | tee Build.log`
 - Check Build.log for any error/problem
 - The newly built firmware in `image/TEW-652BRP_ap81_image.bin`

TEW-652BRP hacking

- Load/upgrade firmware
 - Connect to the router (via wired ethernet, not wireless)
 - Do not upgrade firmware over wireless
 - Go to Tools->Firmware
 - Upload the new firmware. The router will come back in 2 minutes.

TEW-652BRP hacking

- Directories of interest
 - apps: where the apps (busybox, dnsmasq, etc.) are.
 - You can insert your own app here.
 - platform/AR9100/kernels: where the kernel resides.
 - platform/AR9100/target: where the root file system is built from.
 - You can modify the files in the root file system here.
When done, tar jcvf the target directory into rootfs_ap81.tar.bz2. The build will pick up this file for the root fs.

TEW-652BRP hacking

- Modifying/adding app
 - Modify busybox
 - Go to apps/busybox-1.01. Run make menuconfig. Edit (add telnetd), save new .config file as defconfig-ap71.
 - Add your own app (dropbear, etc)
 - Put your app under apps/. Include Makefile to build the app.
 - Modify apps/.config and apps/Makefile files so that the build will pick up your app.

TEW-652BRP hacking

- System startup
 - Look at rootfs/target: this is the root file system directory
 - This firmware uses busybox's init which obeys /etc/inittab
 - Modify etc/rc.d/rcS to get your app started.
 - Put your app's init script in etc/rc.d/

TEW-652BRP hacking

- Alternative
 - Use Firmware Mod Kit
 - http://www.bitsum.com/firmware_mod_kit.htm
 - Run `extract_firmware.sh` to extract the stock firmware
 - Root file system is in `workspace/rootfs`
 - Kernel is in `workspace/vmlinuz`
 - Run `build_firmware.sh` to rebuild the firmware.

TEW-652BRP hacking

- Why?
 - Pros:
 - Firmware already runs on the box. Drivers work.
 - You just need to add your app/tool. This is quicker than waiting for openwrt support.
 - You keep the UI
 - Cons:
 - Firmware includes proprietary app that you can't change.
 - Build tool does not work out of the box.

TEW-652BRP hacking

- Mia (Mom's Internet Access helper)
 - <http://www.avidz.net/mia/>
 - Time based Parental Access Control
 - Granular time slots 24/7
 - Unlimited profiles
 - Easy to use User Interface (Moms friendly)