Encrypted USB Bootloader for AVRs

Originalartikel

Backup

<html> <p>It probably doesn&#8217;t matter much for the hacker who sleeps with a bag of various microcontroller flash programmers under the pillow, but for an end-user to apply a firmware upgrade, convenience is king. These days that means using USB, and there are a few good AVR USB bootloaders out there.</p> <p>But [Dmitry Grinberg] wanted more:&#160;<a href=„http://dmitry.gr/index.php?r=05.Projects&amp;proj=20.%20ModulaR%20BL“ target=„_blank“>the ability to encrypt the ROM images</a> and verify that they haven&#8217;t been tampered with or otherwise messed up in transit. Combined with the USB requirement, that meant writing his own bootloader and PC-side tools. His bootloader will take unencrypted uploads if it doesn&#8217;t have a password, but if it&#8217;s compiled with a key, it will only accept (correctly) encrypted hex files.</p> <p>Since the bootloader, including the USB firmware, is on the hefty side at 3.3 kB, [Dmitry] included hooks to re-use the bootloader&#8217;s USB code from within the target application. So if you were going to use V-USB in your program anyway, it doesn&#8217;t actually take up that much extra space. It&#8217;s a cute trick, but it ties the bootloader and user program together in a way that gives us the willies, without specifically knowing why. Perhaps we can debate this in the comments.</p> <p>If you need an AVR USB bootloader, but you don&#8217;t need the encryption, we like <a href=„https://hackaday.com/2014/03/04/interrupt-free-v-usb/“>Micronucleus</a>. But if you need to deliver updates to users without them being able to modify (or screw up) the code in the middle, give [Dmitry]&#8217;s setup a try.</p> </html>

From:
https://schnipsl.qgelm.de/ - **Qgelm**

Permanent link:
https://schnipsl.qgelm.de/doku.php?id=wallabag:encrypted-usb-bootloader-for-avrs

Last update: **2021/12/06 15:24**