THURSDAY, AUGUST 23, 2007

Some Comments on the Method

This method is very similar to the method used to unlock the Siemens phones with the S-Gold2 chipset. The S-Gold2 has a bootrom which allows you to download a bit of unsigned code. This code is run if certain flash addresses are blank. Using a little hardware trick, which I'll explain later, we make them appear blank. Then once we have unsigned code running on the baseband, we can download a modified firmware, with the unlock patched in, to the nor flash. The signature checks only cover this region while it is being downloaded the first time. Once the code is on the NOR we can do whatever we want. So patch out the PN lock; Voila, unlocked iPhone.

POSTED BY GEORGE HOTZ AT 6:23 AM