

Security for embedded device

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-06/1957.html>

From: Joris Dobbelsteen (*none.of_at_your.business*)

Date: 06/27/04

Date: Sun, 27 Jun 2004 22:28:43 +0200

I'm looking for some good starting point in designing a simple mechanism of preventing a combination of hardware and software to be duplicated or used very widely.

It must prevent hobbyist from putting their own equipment instead of using mine, so its not very demanding in this aspect.

Basically it runs on:

- * PC (or PocketPC) with Windows (CE)
- * Embedded chip (Zilog eZ8 is planned, I love this thing :)).
This thing cannot store any data, which is a limitation.

The basic idea was that the computer needs a specific 'code' to unlock the embedded device and that a unique key is generated to make the unlock not replayable. With this a simple key is generated to encipher the data that actually matters (signal output only).

The other way would be sending the chips serial number (or derived) to the PC so it can do validation. Since I cannot store anything in the embedded chip, it cannot be a neat mutual authentication scheme.

Perhaps anyone has a good point to a simple cipher for a 8-bit processor?
Any other good starting points would be highly appreciated!

Another issue is running the software on the PC, where it should be locked to a single system. Does anyone have a good advice on getting a unique number on a Windows system (preferably something that works under .NET). My last idea was to use the CPUID on the Intels and AMDs or the Windows Product ID if the CPUID isn't available.

Perhaps there is a better alternative or its out of scope here?

– Joris