Code protection and attacks against ATMega series

Dionisio Perez-Mavrogenis

February 8, 2014

This research project will look at the various issues concerned with protecting Intellectual Property(IP) in microcontroller units(MCU)(in this context, IP would refer to an attacker stealing the firmware from the board and replicating it on their own hardware, a situation with multiple consequences). The motivation behind this is the rise of the "Web of things", a notion that everyday devices will have microcontrollers embedded in them in order to make them more reactive and adaptive to a person's life, and their long history of industrial applications.

The research will focus on the ATMega series of boards. The reason for this is that it is an open-source hardware platform and thus information for it is more readily available and it is very popular. Moreover, making the research platform-specific will allow for a deeper understanding of the problems and countermeasures and provide a more engaging research topic, since the focus is not on an idealised hardware platform (however, there is little loss of generality as most boards have a similar structure and thus are affected by the same issues).

The aims of this research is to provide a comprehensive and coherent overview of the current attack vectors and implications in the case of a successful attacker, as well as provide some possible countermeasures to hinder IP unlawful duplication.