Strong password hashing on embedded devices

Francisco Blas Izquierdo Riera, Chalmers University of Technology

Although password based authentication remains one of the most common way to authenticate users and strong password hashing algorithms to slow down attacks against databases do exist, the energy and memory requirements present in most environments prevent using such algorithms. During this talk we will present some of the problems that systems developers have to face when trying to implement such algorithms and will briefly introduce some of the solutions we are working on