Embedded systems are found everywhere from consumer electronics and cars to critical infrastructure and medical devices. And with the growth of the Internet of Things (IoT), these systems are increasingly interconnected. As a result, embedded security is an area of growing concern with potentially life-threatening and socially disruptive impact. Yet research, as well as real-world incidents, continue to demonstrate how vulnerable embedded systems actually are.

The focus of this thesis was binary security, the exploitation and mitigation of memory corruption vulnerabilities. The state of embedded binary security was evaluated by means of the first quantitative and qualitative analysis in literature and several gap areas that were identified showed embedded systems lagging behind their desktop, laptop and server cousins significantly. As a next step the challenges and limitations standing in the way of improvements were identified and the criteria for a minimum baseline outlined. Finally uArmor, the first such baseline, was designed, implemented and evaluated to meet those criteria and serve as a step towards hardening embedded systems against cybersecurity threats.