Abstract

Dynamic Software Updating (DSU) consists in updating running programs on the fly without any downtime. This feature is interesting in critical applications that must run continuously. Because updates may lead to safety errors and security breaches, the question of their correctness is raised. Formal methods are a rigorous means to ensure the high level of safety requested by such applications. The detection of points to perform safe updates is a critical issue in DSU. Indeed, an hazardous update point leads the updated system to erroneous and unexpected behavior. We present in this paper a mechanism to detect safe update points in DSU for Java Card applications. The mechanism is then formally verified using model checking against correctness properties: deadlock free, activeness safety and DSU-liveness.