Part III
RUNTIME VERIFICATION FOR MODERN MICROPROCESSORS
As microprocessor complexity grows with each new generation of products, the capabilities of even the most advanced pre-release (i.e., pre- and post-silicon) verification solutions still severely lags behind, allowing bugs to slip into production hardware and compromise the stability and security of customers’ systems. Because of this, researchers in academia and industry recently started to propose solutions that extend verification and protection from bugs to a deployed processor by means of patching and/or additional on-chip hardware. The purpose of this additional hardware components is to monitor the stability of the system at runtime. In this third part of the book we overview and classify escaped bugs in commercial processors available today, collecting them from publicly available errata report documents. We then present research solutions leveraging hardware checkers to ensure correctness of runtime operation. This introduction is followed by the presentation of a comprehensive solution for patching processors’ hardware in the field and for protecting users from unknown escaped bugs. Following the discussion of techniques to protect individual processor cores, we turn our attention to multi-cores and present one checker-based and one patching-based runtime verification solution for these architectures. In our concluding remarks we recap the state-of-the-art approaches to microprocessor validation and outline future research thrusts that are crucial in closing the verification gap and protecting both manufacturers and end-users from the severe impacts of processor design bugs.