Static Driver Verifier, a Formal Verification Tool for Windows Device Drivers

Vladimir Levin
Microsoft Corporation

Microsoft is improving the quality of system software, in particular, through the intensive application of Formal Methods. The ultimate goal is to reach a point at which robustness against failures and attacks can be guaranteed. To support this goal, the company has invested in advanced testing and verification tools. Examples include model-based testing supported by AsmL/Spec#, TLC and Zing model checkers for concurrency verification, a type system augmented with pre-/post-conditions (Fugue), advanced static analysis tools (PreFix, ESP, etc.) and Static Driver Verifier, SDV.

SDV is a formal verification tool aimed at checking device drivers developed using the Windows Driver Model (WDM) interface. The WDM interface consists of more than 800 functions - entry points into the kernel functionality. To correctly use the WDM interface is not easy: WDM rules are numerous and complicated.

SDV is based on the Slam engine which model checks a C program against a safety property written in Slic. Slic is a language for describing safety automata over events associated with entries into and exits from C procedures. A vast majority of WDM rules can be expressed in Slic in a generic manner - i.e. a WDM rule can be written in Slic as a single property that should hold on every WDM device driver.

A lightweight analysis of a driver’s C code and a rule-tuning script are also packaged into SDV, as well as a predefined set of WDM rules written in Slic. With this package, SDV can be used as “a push button tool”: the user issues the command staticdv in the directory with her device driver and the driver is model-checked against the 85 predefined WDM rules. If errors are found then a source-level browser appears for browsing error traces.

In Microsoft, SDV has been used for debugging device drivers since the spring of 2003. In November 2003, SDV was demonstrated at the Driver Developer Conference in Redmond, WA. Attendees ran SDV on device drivers they brought. This year, we intend to release SDV for use by third-party driver developers.

More information about Slam and SDV can be found on http://research.microsoft.com/slam.