Finding bugs in device drivers with Static Driver Verifier

Byron Cook

Microsoft Research

Abstract. Bugs in kernel-level device drivers are one of the leading causes of system crashes in the Windows operating system. Many of these bugs are due to cases in which device drivers fail to maintain the many subtle internal kernel invariants or follow the complicated kernel API calling conventions. Finding these bugs during testing is difficult because they often do not result in immediate crashes. Instead, these flaws put the kernel into an inconsistent state which can then result in erroneous behavior later in the system's execution. Additionally, because drivers execute in a open and concurrent environment and often interact with hardware, it is difficult to achieve adequate coverage during testing.

In this talk we introduce Static Driver Verifier (SDV)—a tool that automatically finds violations of API usage rules in Windows device drivers. SDV is the packaging of a set of API usage rules together with the SLAM software model checker.

This is joint work with Thomas Ball, Vladimir Levin, Jakob Lichtenberg, and Sriram K. Rajamani