

Righting Software

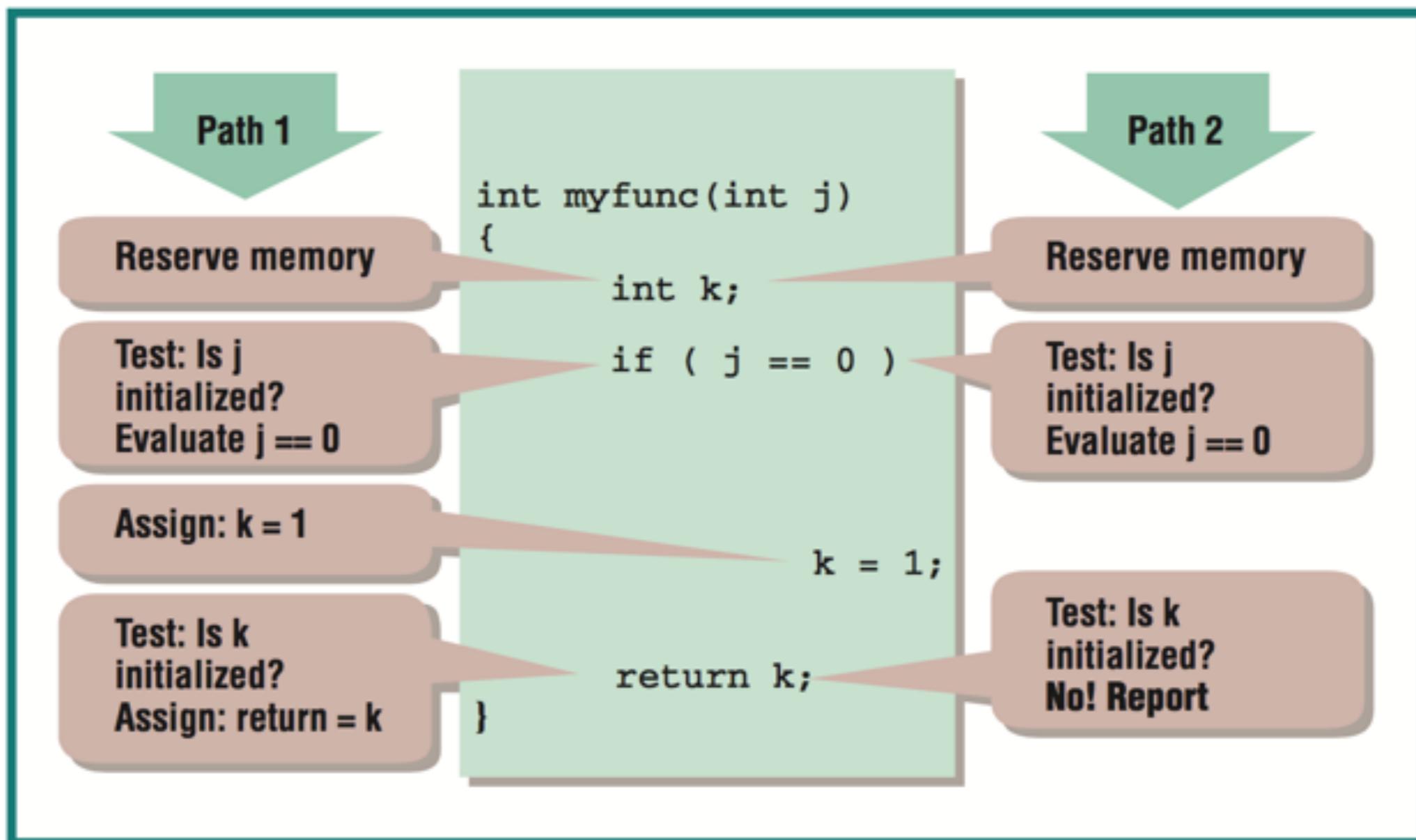
James R. Larus, Thomas Ball, Manuvir Das, Robert DeLine,
Manuel Fähndrich, Jon Pincus, Sriram K. Rajamani, and
Ramanathan Venkatapathy
IEEE Software, May-June 2004

Summary by Prof. Thomas LaToza
SWE 795, Spring 2017
Software Engineering Environments

Detecting Errors with Static Analysis

- Goal: Find important defects through static analysis.
 - Errors in using PL features such as referencing uninitialized variable
 - Errors in API usage such as closing a file descriptor twice
- NOT to determine that program definitely behaves as expected
 - Only to rule out programs that are obviously buggy

Key Idea: Path Exploration



Challenge: Path Feasibility

```
FILE* f;  
if (complex_calc1())  
    f = fopen(...);  
...  
if (complex_calc2())  
    fclose(f);
```

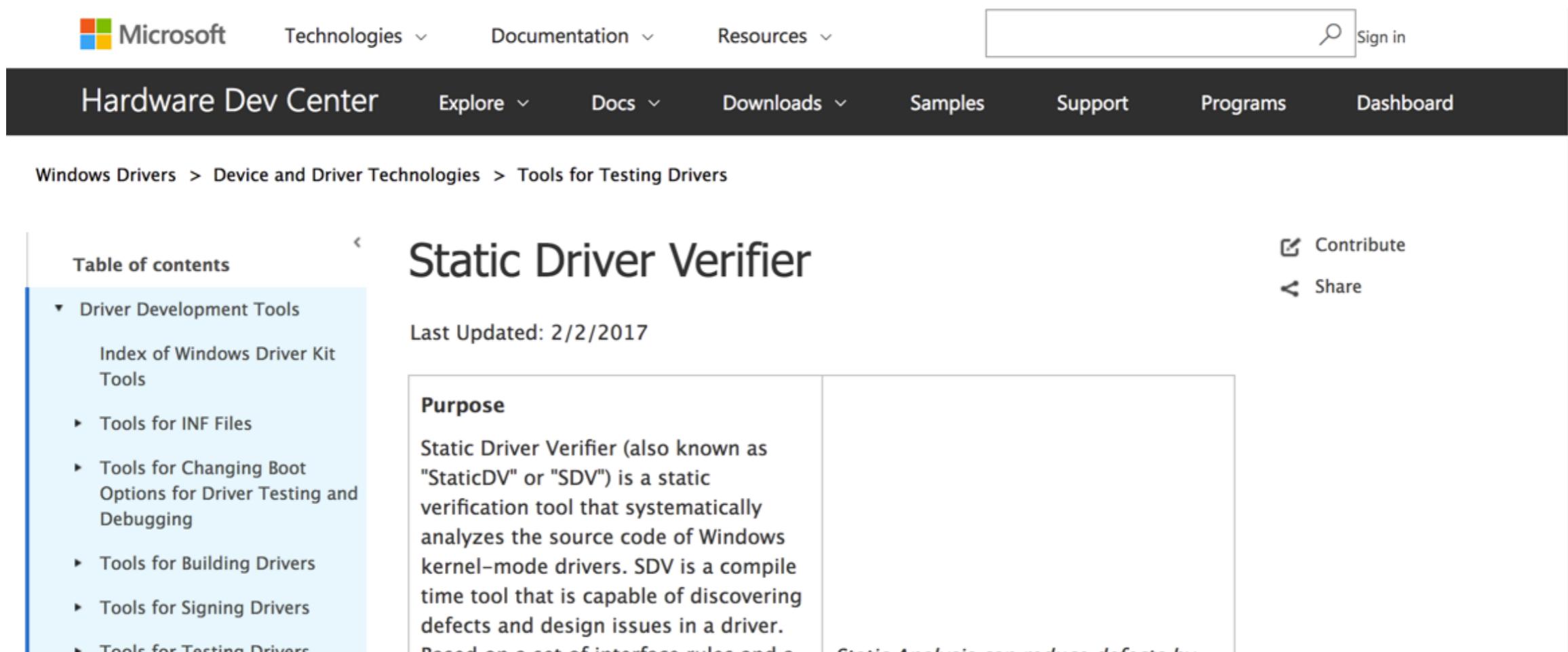
- Determining if path is feasible is hard
- Can't always succeed
- What happens when you don't?
 - Show an error that might be spurious (Sound)
 - Don't show an error that might be spurious (Complete)
 - Show an error if you're fairly confident (Heuristics)

(Some) MS Static Analysis Tools

- Prefix—traverse interprocedural paths, builds models of functions, limit # of paths & use heuristics
- Prefast—use local intraprocedural analysis to find idioms such as wrong param values
- Slam—find protocol violations by building & refining Boolean program abstractions
- ESP—less precise, more scalable interprocedural analysis by pruning irrelevant branches
- Valut—safe version of C that enables modular checking by adding annotations

History

- Tools initially built in late 90s and 2000s at Microsoft
- Used widely internally & in some cases externally (e.g., device drivers)
- Slam tool credited with helping reduce blue screens in MS Windows (other innovations helped too)



The screenshot shows the Microsoft Hardware Dev Center website. The top navigation bar includes links for Microsoft, Technologies, Documentation, Resources, a search bar, and a sign-in button. Below the bar, a secondary navigation bar features links for Hardware Dev Center, Explore, Docs, Downloads, Samples, Support, Programs, and Dashboard. The main content area displays the 'Static Driver Verifier' page, which is part of the 'Tools for Testing Drivers' section under 'Driver Development Tools'. The page includes a 'Table of contents' sidebar with links to various driver development tools. The main content area is titled 'Static Driver Verifier' and includes a 'Last Updated: 2/2/2017' timestamp. A 'Purpose' section describes SDV as a static verification tool that analyzes kernel-mode drivers for defects and design issues. The page also includes 'Contribute' and 'Share' buttons.

Microsoft Technologies Documentation Resources

Sign in

Hardware Dev Center Explore Docs Downloads Samples Support Programs Dashboard

Windows Drivers > Device and Driver Technologies > Tools for Testing Drivers

Table of contents

- Driver Development Tools
 - Index of Windows Driver Kit Tools
 - Tools for INF Files
 - Tools for Changing Boot Options for Driver Testing and Debugging
 - Tools for Building Drivers
 - Tools for Signing Drivers
 - Tools for Testing Drivers

Static Driver Verifier

Last Updated: 2/2/2017

Purpose

Static Driver Verifier (also known as "StaticDV" or "SDV") is a static verification tool that systematically analyzes the source code of Windows kernel-mode drivers. SDV is a compile time tool that is capable of discovering defects and design issues in a driver. Based on a set of interface rules and a

Contribute Share

Questions for discussion

- Overall reaction to the paper
- Would you use such a system for your everyday programming?
 - Why or why not?
- In what circumstances are these tools most useful?