Introduction

- Much system software is configurable at compile-time
- In fact in two worlds: configuration ↔ implementation
  (in Linux: 10,000 Kconfig items ↔ 80,000 #ifdef blocks)
- This is prone to inconsistencies
  → configurability defects → bugs

Problem Analysis

- Two flavors of configurability defects:
  1. Symbolic defects → integrity violation wrt. feature identifiers
  2. Logic defects → integrity violation wrt. feature constraints
- Two confirmed examples, found by our tool:

Our Approach

- Configuration space constraints
- Implementation space constraints
- Configurability defects

Realization: The Undertaker Tool

- Mission: The undertaker finds dead and undead feature code
  (in order to bury it, eventually!)
- Find 1776 defects in Linux 2.6.35; on this basis we have
  - Proposed a fix for 364, among them 23 bugs (22 new)
  - Removed 5129 lines of superfluous #ifdef cruft from the source
  - So far 123 patches submitted (15 acked, 49 merged, 36 pending)

Results and Conclusion

- Conclusion: Configurability is a significant and underestimated source of bugs in system software!