Clang/LLVM for Automated Defense

John Criswell

University of Illinois at Urbana-Champaign

Automated Defense

A compiler that automatically generates executables that are protected against one or more broad classes of attacks.

Trouble on the Horizon

- We *depend* on **vulnerable** computing systems
- Attackers are better funded and more motivated
- We can't fix all the bugs
- Automated defense can help defend us

Clang Has Automated Defenses

- Stack Canaries are bypassed by students for homework
- Partial bounds checks aren’t comprehensive

Potential Ways Forward

System	Overhead
Control Flow Integrity (CFI)	8%
Write Integrity Testing (WIT)	18%
SAFECode (PLDI 2006)	30%
Baggy Bounds Checking	68%
SoftBound + CETS	116%

Note: Table is ***not*** comprehensive.

http://sva.cs.illnois.edu/menagerie

From Research to Practice

- Stop trying to use weak solutions
- Use best of breed techniques
- Realistic discussions of security/performance tradeoffs
- Build what people need