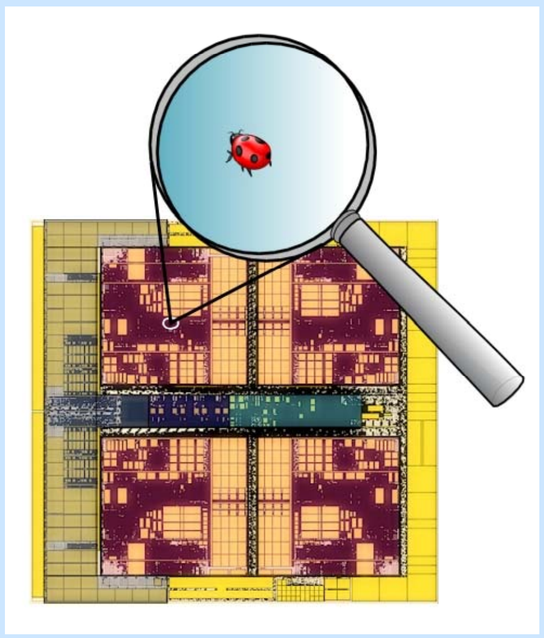
Formal Verification for Secure Systems

Warren A. Hunt, Jr. and J Strother Moore

Trusted Certification Tools
Grant No. CNS-0429591



The ACL2 theorem proving system provides a framework for formal verification that has been applied successfully to a large range of applications, from abstract mathematics to digital hardware designs. In particular, it continues to be used in industry for the verification of security, safety, and correctness properties of commercial computing systems. ACL2 is currently in use in verification efforts for network security properties, cryptographic algorithms, and security-critical digital hardware designs.

ACL2 Customers

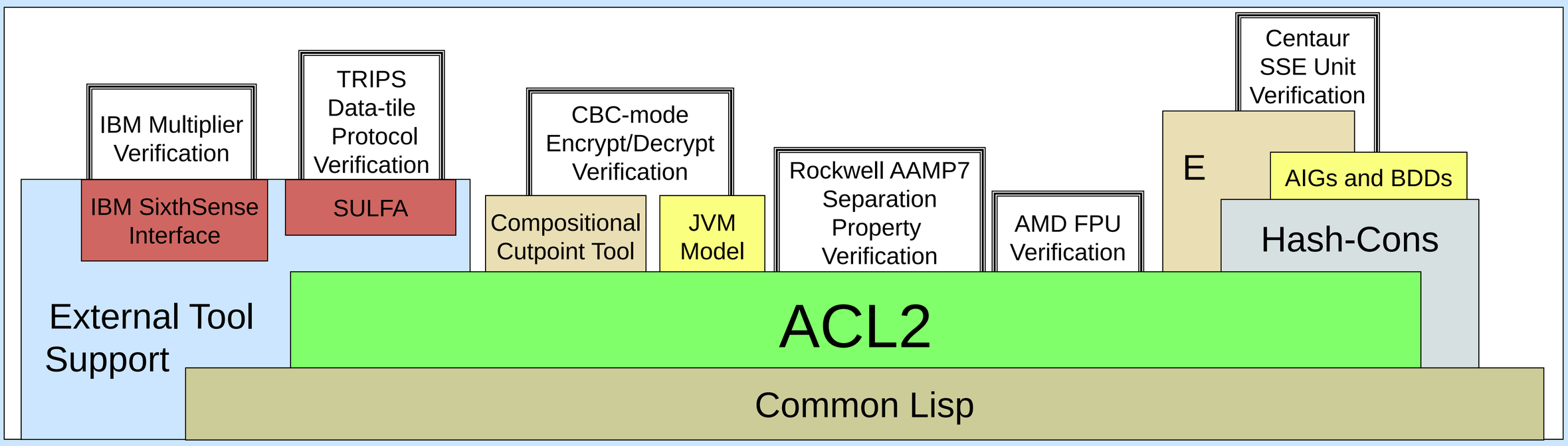
AMD
Boeing
Galois
IBM
Intel
Johns Hopkins
JPL
Microsoft
National Instruments
NSA
Rockwell Collins
w3.org

Generic Proof Tools

Special-purpose frameworks support functional and non-functional (e.g., information-flow) analysis of machine code, thus allowing the user to focus on the “interesting” proof obligations. This methodology has been used to prove the invertibility of a JVM implementation of a CBC-mode encryption/decryption algorithm.

Flexible Tools for Digital System Verification

The E hardware modeling language provides a framework for specification, modeling, and the application of multiple verification methods to prove that a hardware model, or any FSM, satisfies its specification. At Centaur Technology, this is being used to verify an SSE floating-point unit, used in cryptographic applications.



User-definable Proof Tactics

The ability to extend ACL2 with other reasoning tools (both verified and unverified) allows users to build application-specific approaches tailored for their verification tasks and to call external tools for specialized kinds of reasoning.

Fast Executable Logic

ACL2 functions are executable in Common Lisp, making possible proofs by execution of verified decision procedures. The hash-cons extension allows the introduction of transparently memoized functions with no additional logical complexity.

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Cyber Trust Principal Investigators Meeting
March 16-18, 2008
New Haven, CT

THE UNIVERSITY OF TEXAS AT AUSTIN
WHAT STARTS HERE CHANGES THE WORLD