TECHNISCHE UNIVERSITÄT DRESDEN

Certified Verification of Security Properties for Multicore Architectures

Hendrik Tews

Chair of Operating Systems, TU Dresden
www.tudos.de

Research at TUDOS

- microkernel based systems
- operating-system verification
- minimal TCB's for security critical applications (Nizza architecture)

Goal

- build high-security software for a multicore smartphone
- prove its security properties
- certify hardware, software and proofs according to EAL10

Formal Methods, Verification

- ultimative technology to ensure trust
- multicore verification and security properties are still research challenges
- expensive; need funding to establish verification standards
- need European know-how to stay competitive

Certification according to Evaluation Assurance Levels

- currently, highest level EAL7 is *without* source code verification
- need new levels for
  - verified source code
  - verified object code
  - trustworthy proofs in trustworthy formal method tools