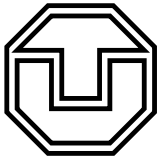
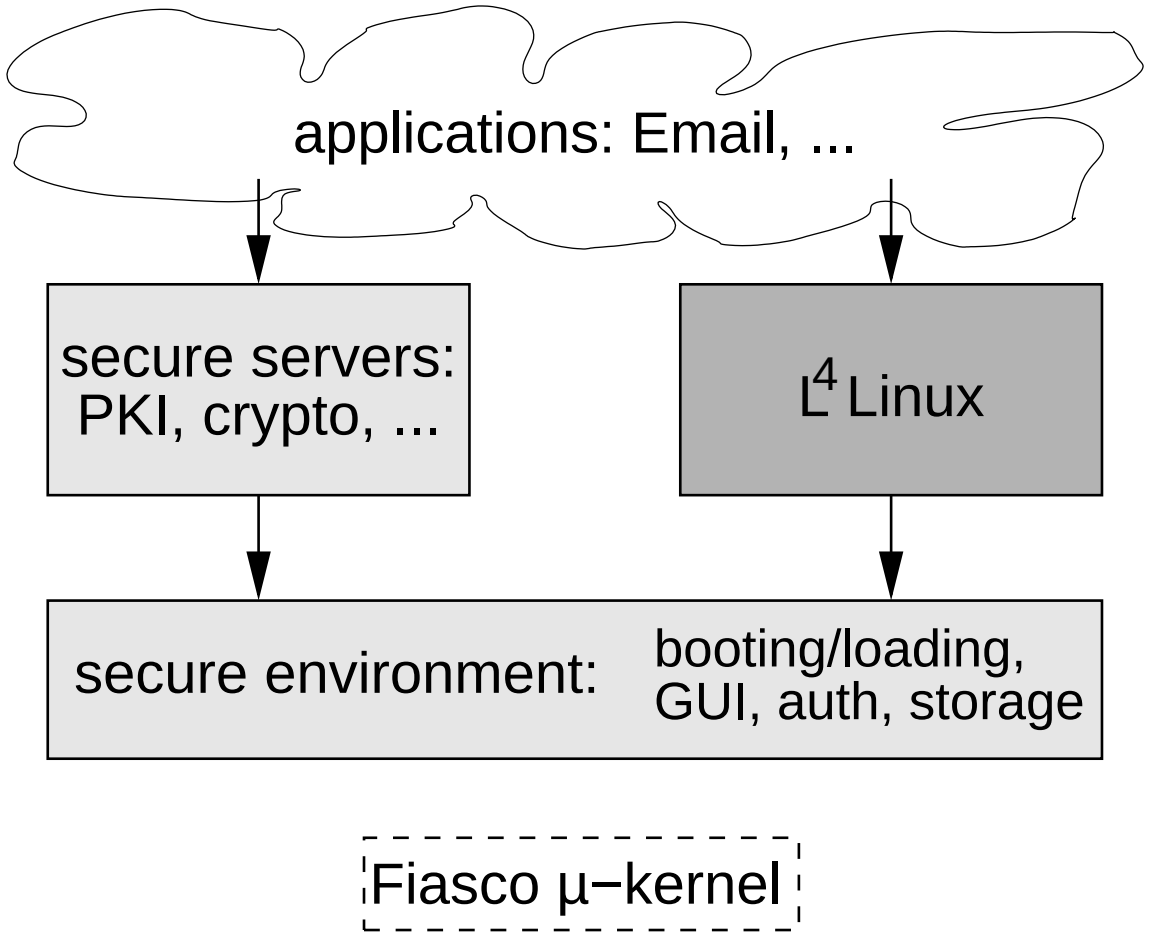
# VFiasco — Towards a provably correct microkernel

Michael Hohmuth Hendrik Tews

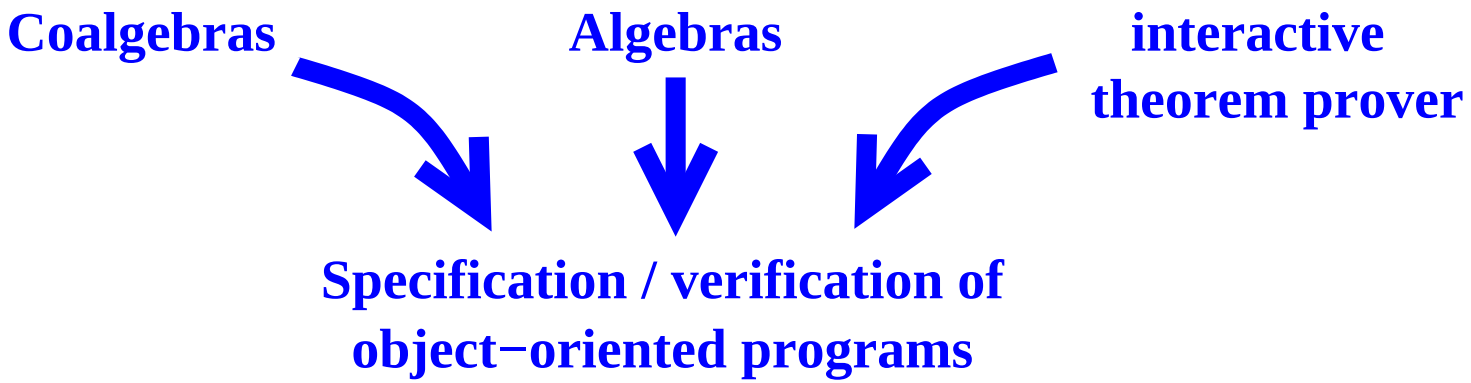


Dresden University of Technology
Department of Computer Science

# Secure microkernel-based systems



# Logic for Object-Oriented Programming (LOOP)




- Nijmegen – Dresden since ’97
- Object-oriented specification / verification
- OO specification language CCSL
- Semantics of Java / JavaCard / JML
- Support for PVS / Isabelle

## Fiasco Case Study

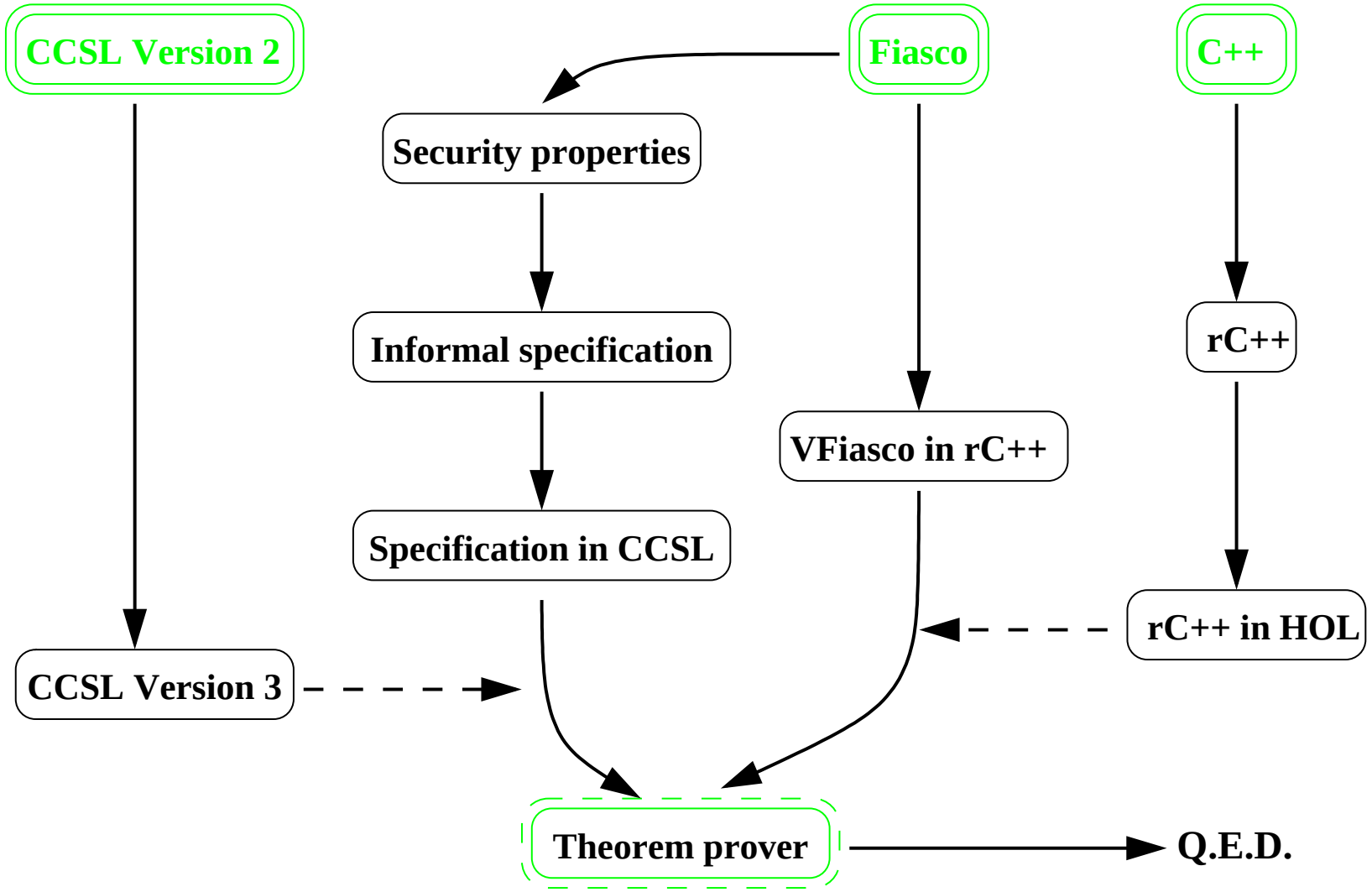
- Specified the interface of class `space_t`
- Checked the C++ source code of `space_t` against the specification

$\Rightarrow$ insertion of superpages proved correct

$\Rightarrow$ verification revealed hidden assumptions

- 4 man months
- CCSL / PVS is ready for operating system verification

# Secure microkernel-based systems



## Summary

- VFiasco project: A formally verified microkernel
- Sounds insane, but case study indicates it's possible
- **VFiasco project:**
  **`http://os.inf.tu-dresden.de/vfiasco/`**
- Case study:
  `http://wwwtcs.inf.tu-dresden.de/~tews/vfiasco/`
- LOOP:
  `http://www.cs.kun.nl/~bart/LOOP/`