Secure microkernel-based systems

applications: Email, ...

secure servers: PKI, crypto, ...

secure environment: booting/loading, GUI, auth, storage

Fiasco µ−kernel

http://os.inf.tu-dresden.de/vfiasco/
Logic for Object-Oriented Programming (LOOP)

Coalgebras \rightarrow Algebras \rightarrow Specification / verification of object-oriented programs

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

http://os.inf.tu-dresden.de/vfiasco/
Fiasco Case Study

- Specified the interface of class `space_t`
- Checked the C++ source code of `space_t` against the specification
  - insertion of superpages proved correct
  - verification revealed hidden assumptions
- 4 man months
- **CCSL / PVS is ready for operating system verification**
Secure microkernel-based systems

CCSL Version 2

Security properties

Informal specification

Specification in CCSL

CCSL Version 3

Fiasco

VFiasco in rC++

C++

rC++

rC++ in HOL

Theorem prover

Q.E.D.

http://os.inf.tu-dresden.de/vfiasco/
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/](http://os.inf.tu-dresden.de/vfiasco/)

- Case study:
  - [http://wwwtcs.inf.tu-dresden.de/~tews/vfiasco/](http://wwwtcs.inf.tu-dresden.de/~tews/vfiasco/)

- LOOP: