Free online textbook series

Formalized in Rocq

Keep it simple

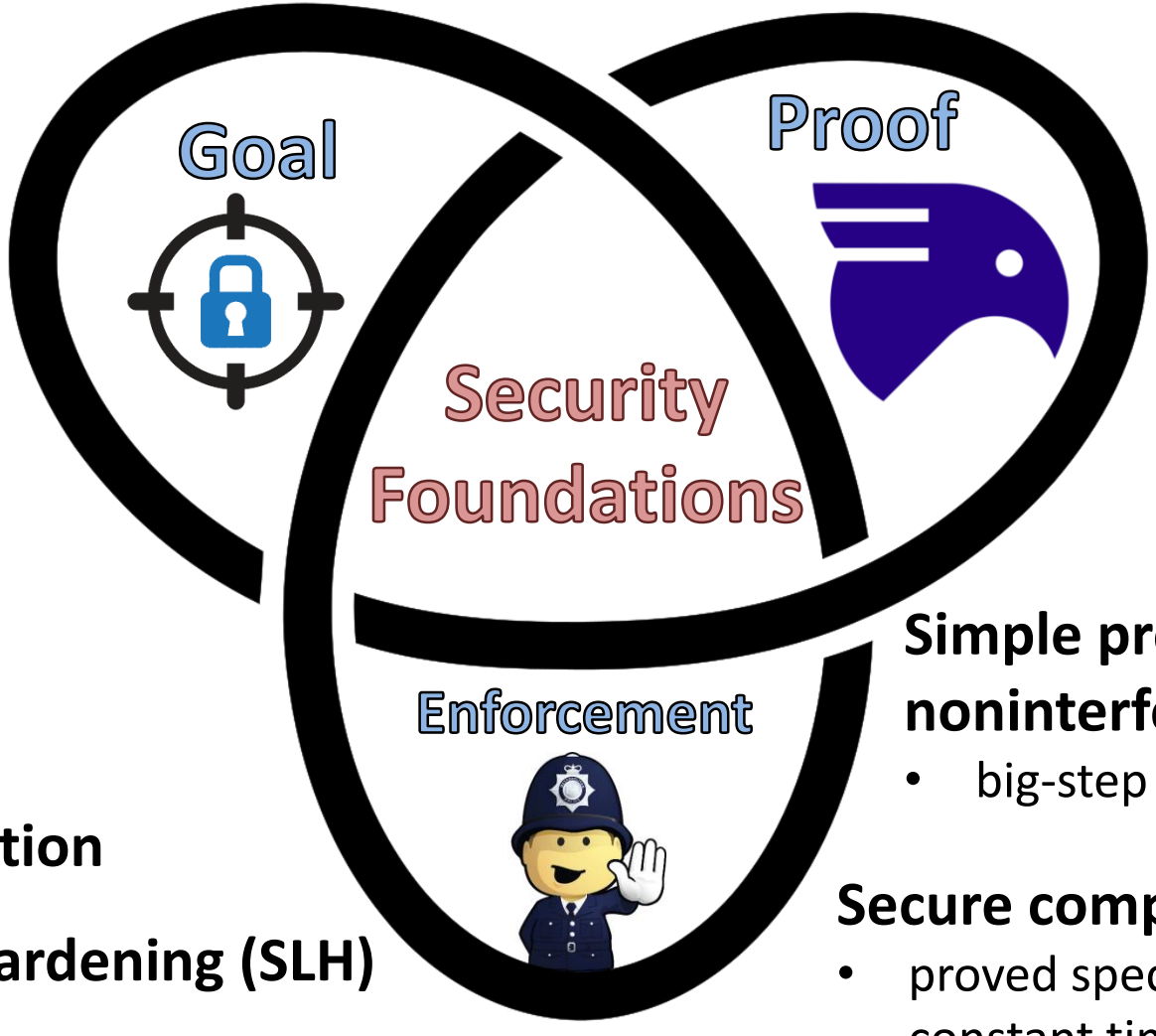
Interactive

Exercise based

New volume on Security Foundations

Noninterference

- for Rocq functions
- stateful commands (Imp language)
- explicit outputs
- side-channels (constant time)



Type systems

Secure Multi-Execution

Speculative Load Hardening (SLH)

WIP: Relational Hoare Logic (RHL)

Simple proofs of noninterference

- big-step

Secure compilation

- proved speculative constant time for SLH [IEEE SP'23]