



Tutorial material and installation instructions available from  
**<https://gitlab.mpi-sws.org/msammler/refinedc-tutorial>**  
(not necessary for following this presentation)

# RefinedC

Automating the Foundational Verification  
of C Code with Refined Ownership types



3.4.2022

VerifyThis 2022

Widely used in industry  
and in high-assurance  
systems



Notoriously prone to  
bugs and security  
vulnerabilities

Formal  
verification to  
the rescue!

# C verification tool desiderata

## Automated

- + Reduces proof
- + Specification
- Large TCB

## Foundational

es proof

Can we get the best  
of both worlds?

Examples:

Verifast, VCC, Frama-C, ...

Examples:

VST, CertiKOS, seL4, ...

# RefinedC

Automated

Guide proof search  
via a type system

Foundational

Semantic model  
in Coq / Iris

$\Gamma \vdash e : \tau$



Ownership types

Handle pointers and  
memory management

Refinement types

Handle functional  
correctness

# RefinedC

Available at

<https://plv.mpi-sws.org/refinedc/>

Automated

$\Gamma \vdash e : \tau$

Foundational

