SECOMP

ătălin Hrițcu

Principal investigator: Cătălin Hrițcu

[2005-2011] Saarland University, Saarbrücken, Germany

[2011-2013] University of Pennsylvania, USA

[2013-now] INRIA Paris, France

- Publications

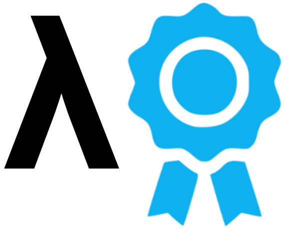
Best venues in security and programming languages

Software Foundations

- Currently supervising 2 PhD and 3 MSc students

- General chair

- PC member



My Research

Devising formal methods

•
•
•
•
•

Solving security problems

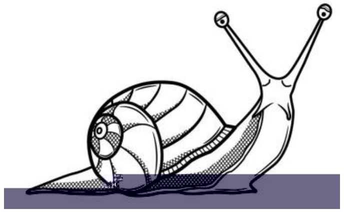
•
•
•
•
•

Resulted in many innovative tools

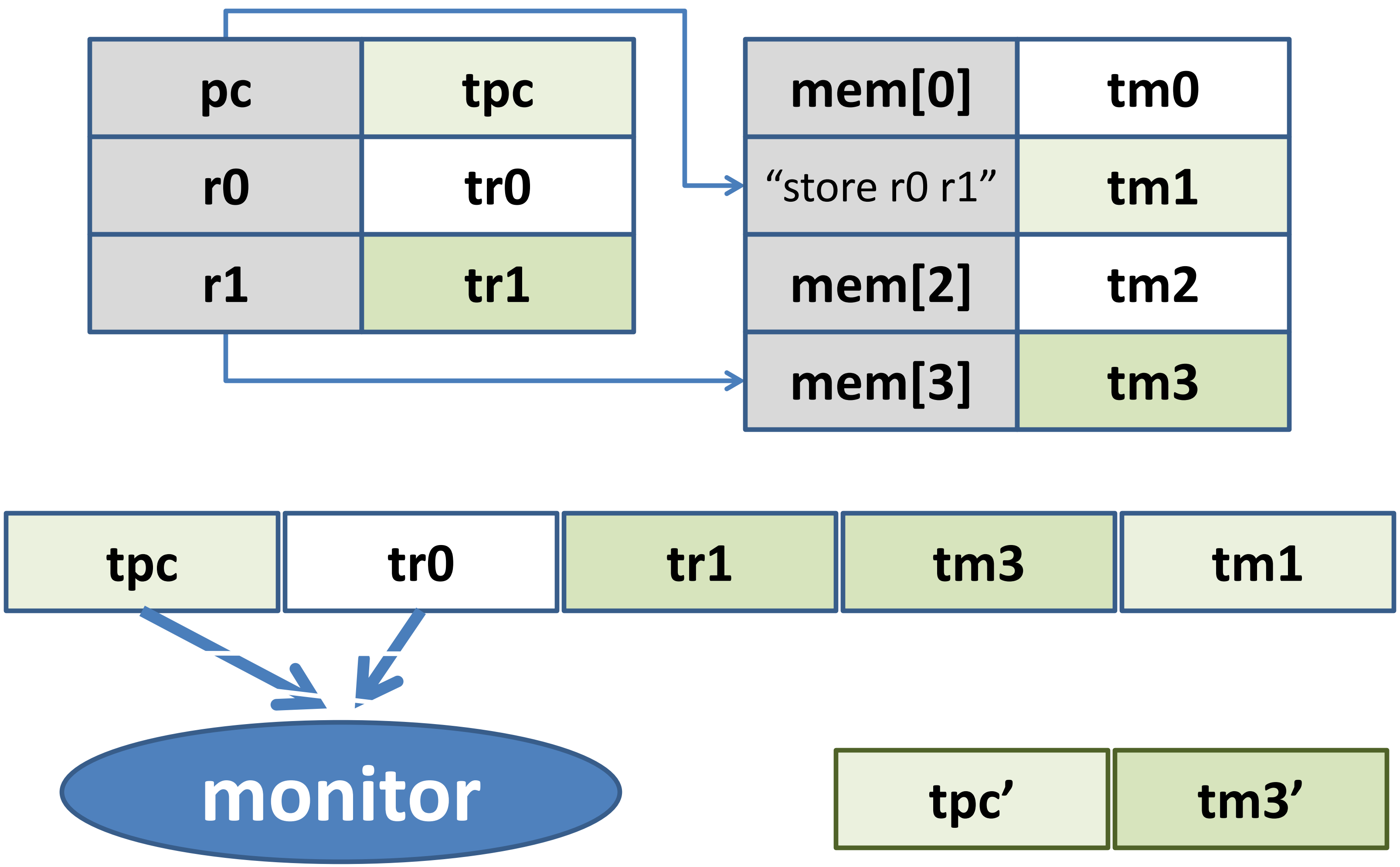
•

The problem: devastating low-level attacks

- 1. inherently insecure low-level languages (C, C++)
  - memory unsafe
- 2. unsafe interoperability with lower-level code
  - safer high-level languages (Java, C#, OCaml)
    insecure low-level libraries (C, C++, ASM)
  - unsafe interoperability:
- Today's languages & compilers plagued by low-level attacks
  - main culprit: hardware provides no appropriate security mechanisms
  - too inefficient

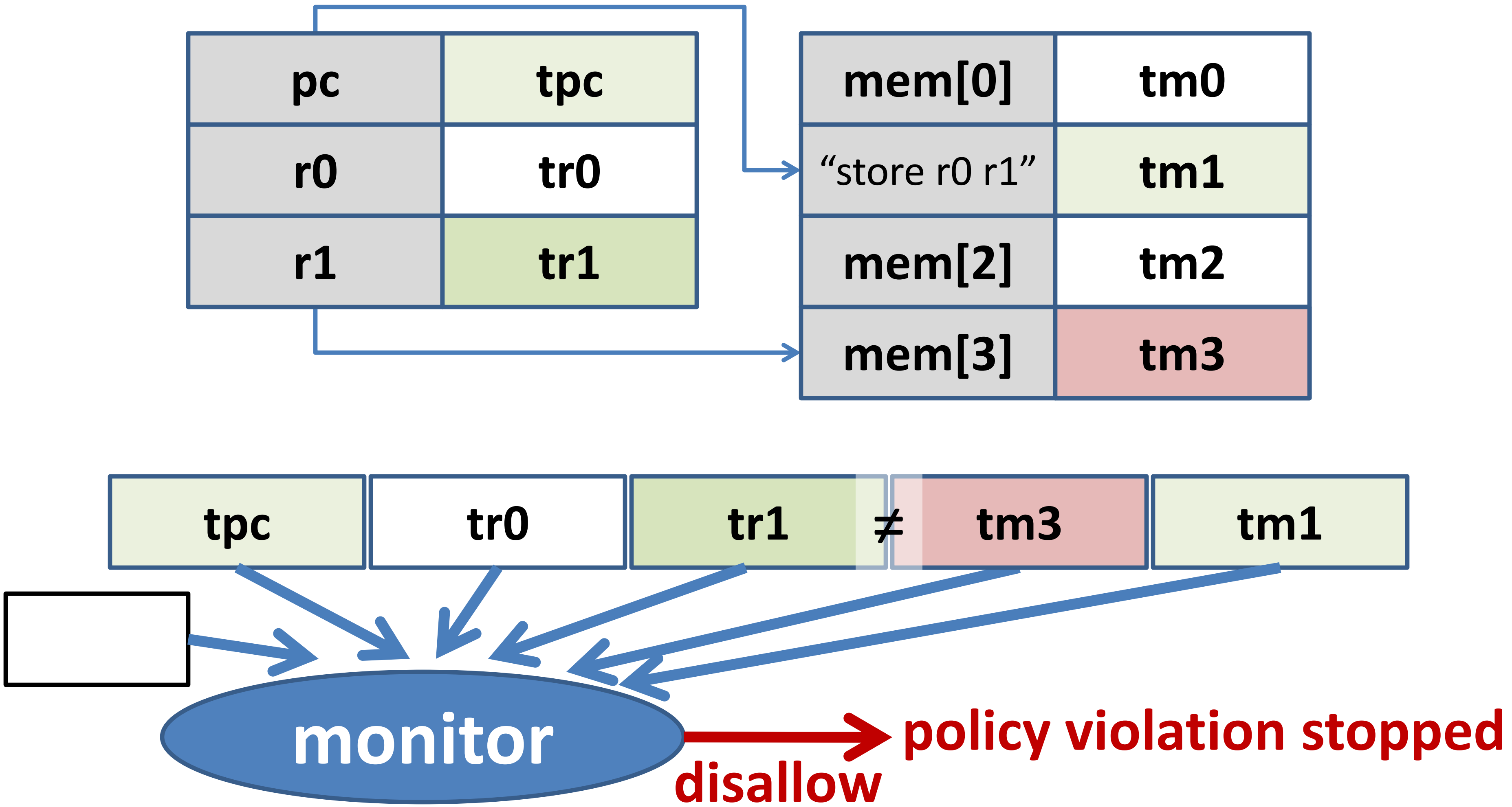


Key enabler: Micro-Policies



Key enabler: Micro-Policies

[Oakland '13 & '15 POPL '14 ASPLOS '15

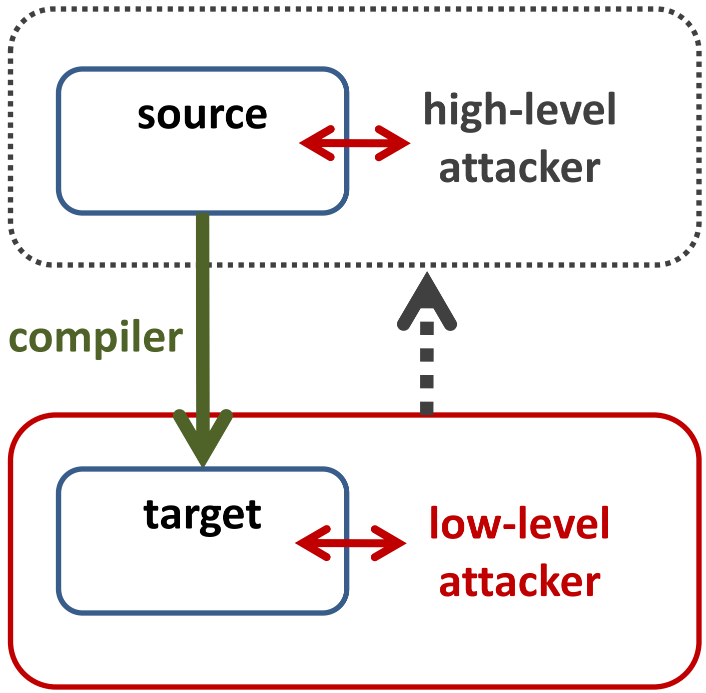


SECOMP grand challenge

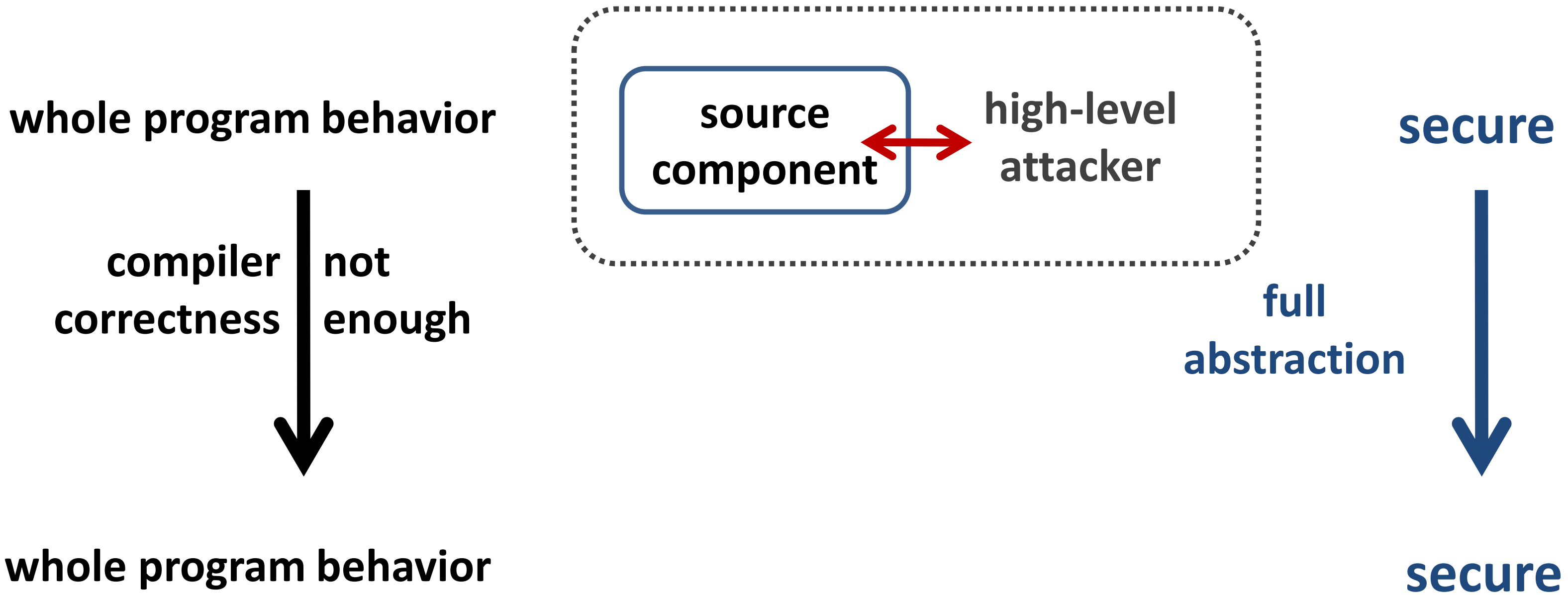
the first efficient formally secure compilers
realistic programming languages

1. **Provide secure semantics for low-level languages**
   –
2. **Enforce secure interoperability with lower-level code**
   – ASM, C, and F* [F* = ML + verification, POPL '16]

Formally verify: full abstraction



Formally verify: full abstraction



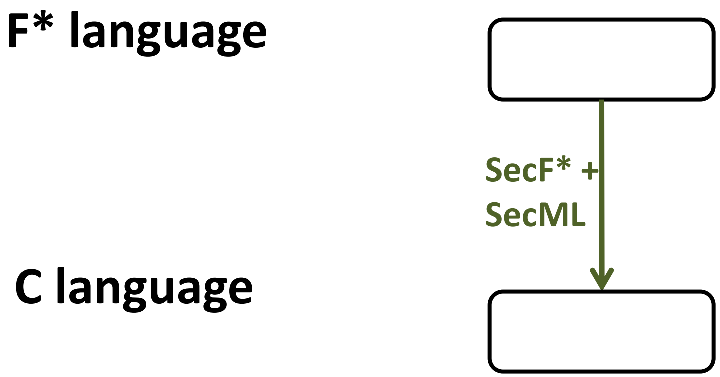
Benefit sound security reasoning in the source language

SECOMP: achieving full abstraction at scale

F* language

C language

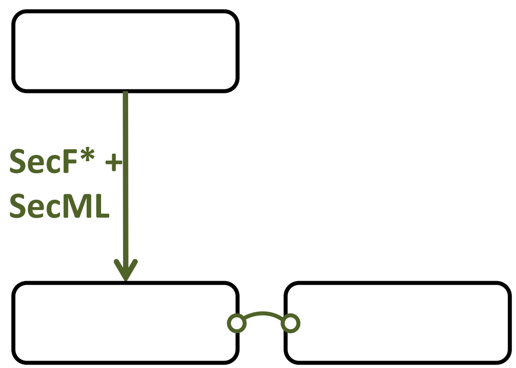
SECOMP: achieving full abstraction at scale



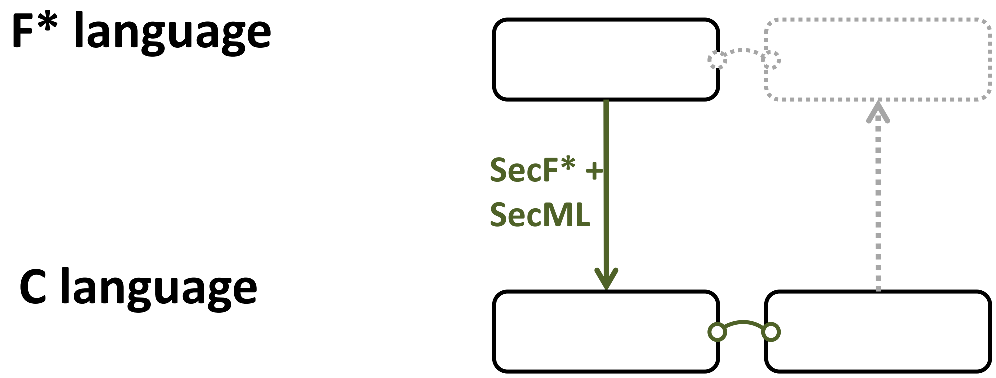
SECOMP: achieving full abstraction at scale

F* language

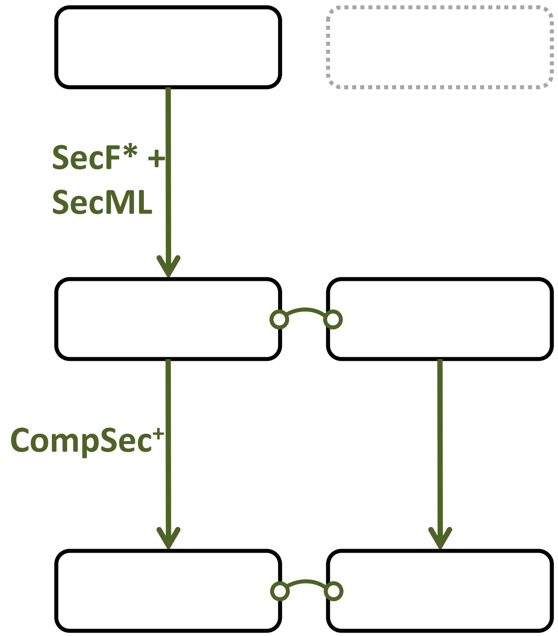
C language



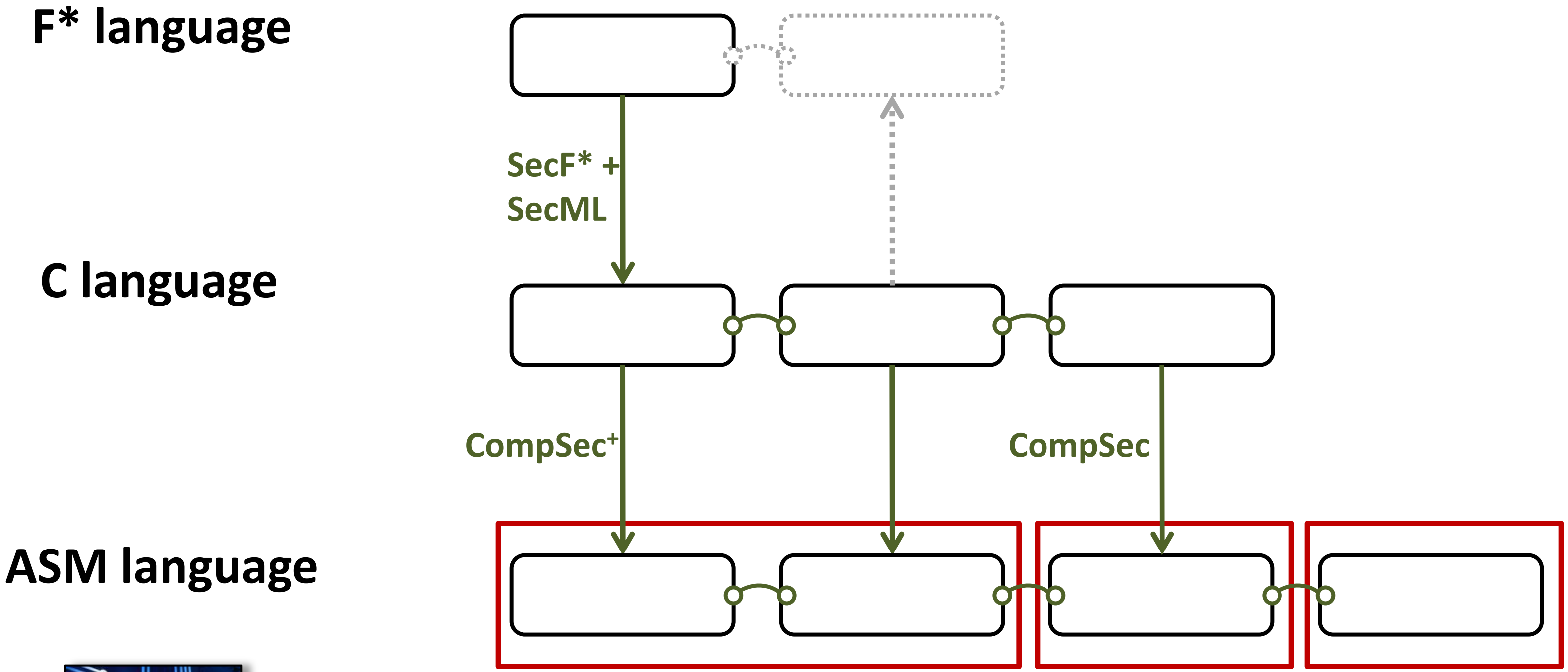
SECOMP: achieving full abstraction at scale



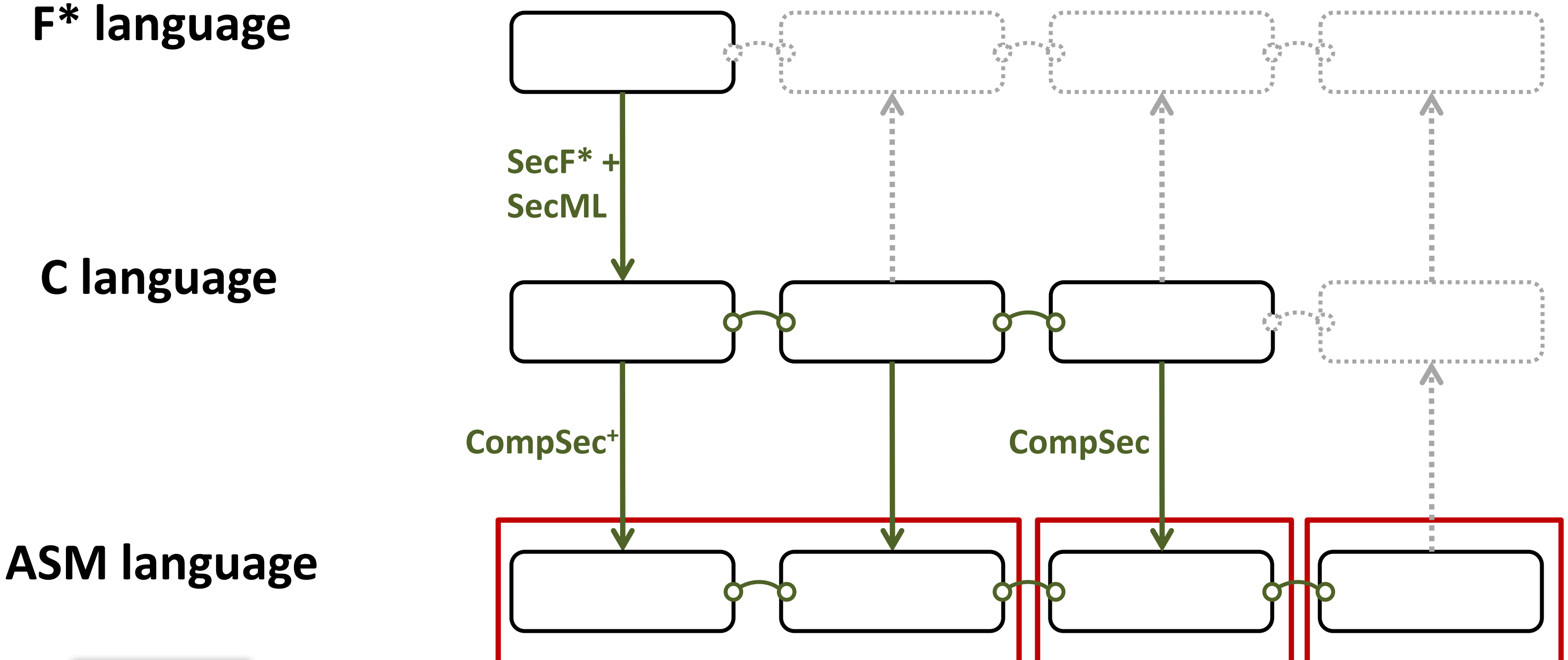
SECOMP: achieving full abstraction at scale



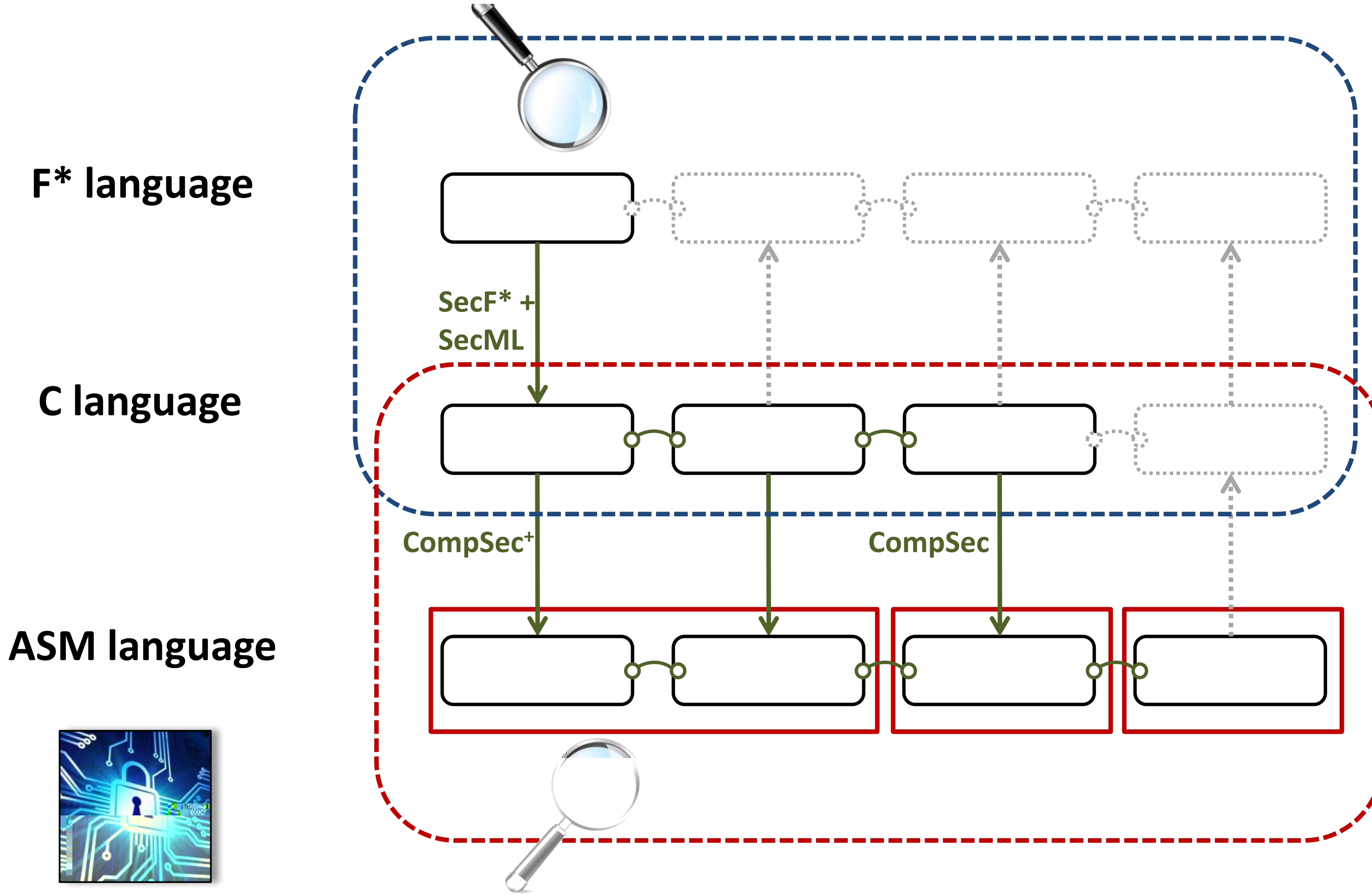
SECOMP: achieving full abstraction at scale



SECOMP: achieving full abstraction at scale



SECOMP: achieving full abstraction at scale



Protecting component boundaries

- Add mutually distrustful components to C
  - strictly enforced interfaces
- CompSec compiler chain
  -
- Micro-policy simultaneously enforcing
  -
  -

- Fundamental challenge: Proper attacker model

ț

Protecting higher-level abstractions

- **Enforcing more interesting abstractions**
  - –
  - –
- **Fundamental challenge: Micro-policies for C and ML**
  - –
- **Fundamental challenge: Secure micro-policy composition**
  - policy's behavior can break another's guarantees

SECOMP research team

- Cătălin Hrițcu (principal investigator, 75%)
- ERC: 1 Junior Researcher, 2 PostDocs, 3 PhD students
-

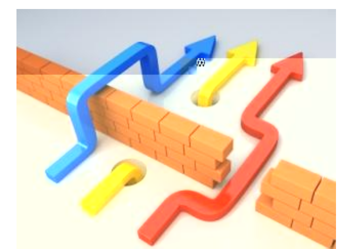
WP	Year 1	Year 2	Year 3	Year 4	Year 5
μ					
μ					

Collaborators & Community

- Ongoing projects
  - Micro-Policies:
  - F* and miTLS*:
  - CompCert:
- New potential collaborators
  - secure compilation
    -
- Secure compilation workshop
  - build larger research community, identify open problems, bring together communities

SECOMP in a nutshell

- We need more secure languages, compilers, hardware
- Key enabler: micro-policies
- Grand challenge: the first efficient formally secure compilers realistic programming languages
- Answering challenging fundamental questions
  –
- Achieving, testing, and proving full abstraction



- Very ambitious and risky milestone project, but ...
  –
- Impact: unprecedented security, could become mainstream