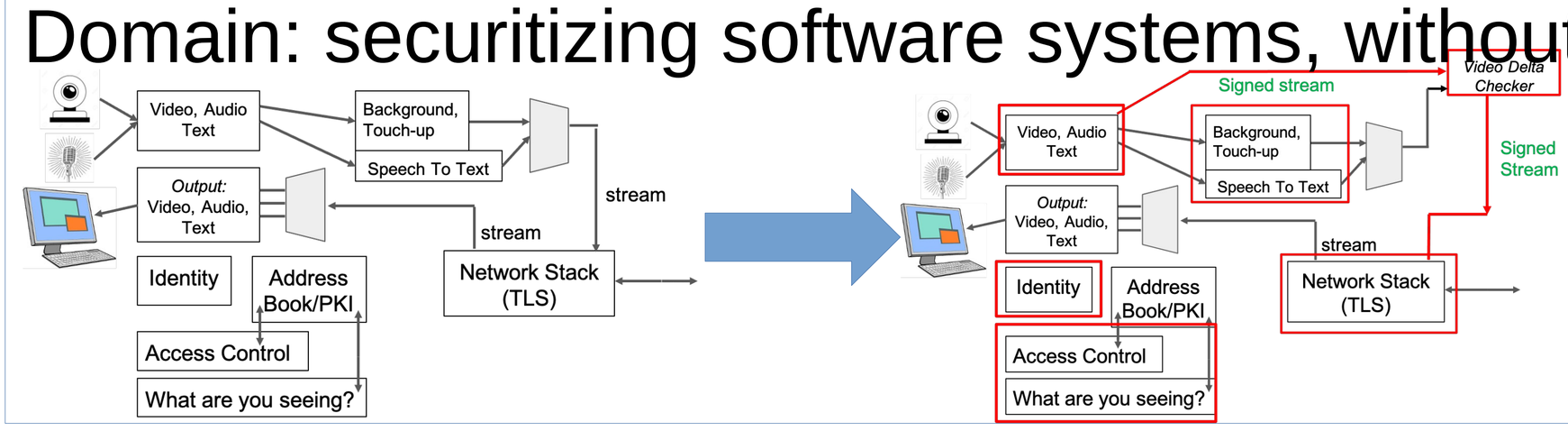
Provably Secure, Usable, and Performant Enclaves in Multicore Processors

PI Prof. Srini Devadas, co-PI Prof. Arvind, co-PI Prof. Adam Chlipala, MIT

Domain: securitizing software systems, without trusting OSes



- Usable APIs
- High performance
- Formal assurance

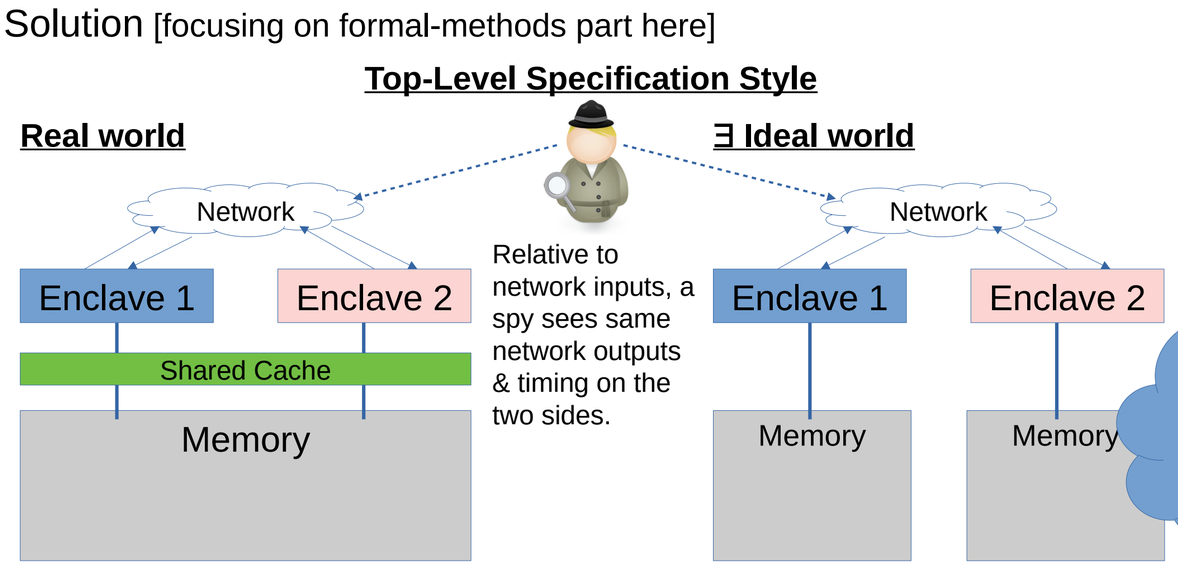
Challenges

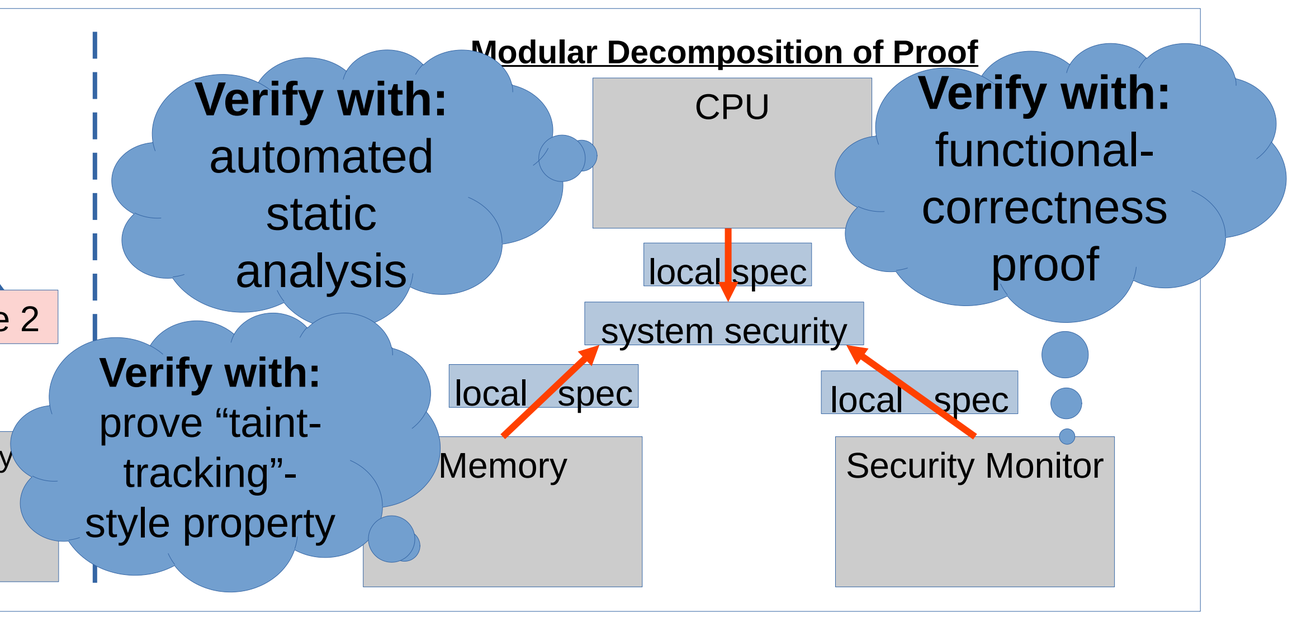
- Addressing all timing side channels
- Trading off between ease of use and security guarantees in APIs
- Maintaining classic microarchitectural optimizations and adding new ones, while providing strong security
- Developing cost-effective formal-verification techniques

Scientific Impact

- New design principles in secure software APIs that avoid timing-channel leaks
- New architectural & microarchitectural ideas relevant to secure systems
- New formal-methods approaches to decompose analysis modularly, with timing-sensitive specifications

Solution [focusing on formal-methods part here]





Real-world impact

- Platforms for secure app development
- Open-source releases of enclave system (hardware + software), ready to deploy on AWS FPGAs, for penetration testing and extension

Education

- Extensions to MIT's graduate classes on computer & network security and computer architecture
- Made freely available via Open Courseware platform

Broader Participation

- Supporting MIT's PRIMES and PRIMES Circle programs
  - PRIMES Circle: introducing computing to HS students from underrepresented groups
  - PRIMES: research projects for HS students who progress far enough