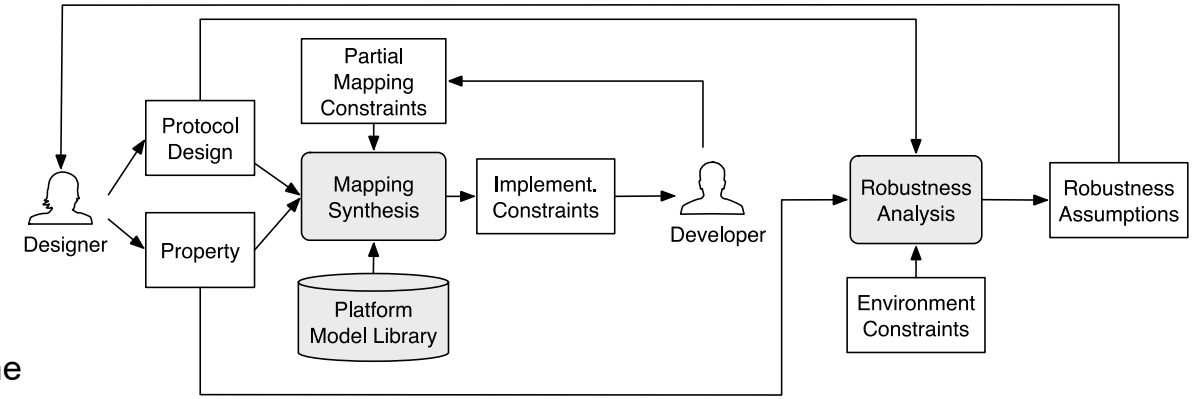
SaTC: CORE: Medium: Collaborative: Bridging the Gap Between Protocol Design and Implementation through Automated Mapping

Daniel Jackson (MIT), Eunsuk Kang (CMU), Stéphane Lafortune (University of Michigan), Rômulo Meira-Góes (CMU)
Cristina Nita-Rotaru (Northeastern University), and Stavros Tripakis (Northeastern University)

Challenge:

- Correctly implementing security protocols is challenging, due to the under-specified nature of protocol specifications
- Assumptions made at the spec level may be violated by the underlying implementation platform
- Can we provide tools and techniques for ensuring conformance between the spec and implementation?



Solution:

- A novel protocol development methodology that combines:
- (1) **Mapping synthesis**: A technique for automatically synthesizing mappings from spec to implementation
- (2) **Robustness analysis**: A technique for computing implicit assumptions that the protocol makes about the attacker

Scientific Impact:

- Provide a systematic approach to hardening protocol implementations through generation of secure mappings
- Provide an understanding of security attacks on protocols caused by a violation of implicit assumptions
- Aid developers in identifying such assumptions and improve protocol robustness

Broader Impact and Broader Participation:

- As security protocols form a backbone in today's web infrastructure, improving their robustness is crucial
- Possible transition to practice through improving protocol documentation (e.g., RFCs) by robustness analysis
- Provided research opportunities to undergraduates, PhD students and research fellows

Award numbers: CNS-1801546 (Northeastern), CNS-1801342 (Michigan), CNS-1801399 (MIT)