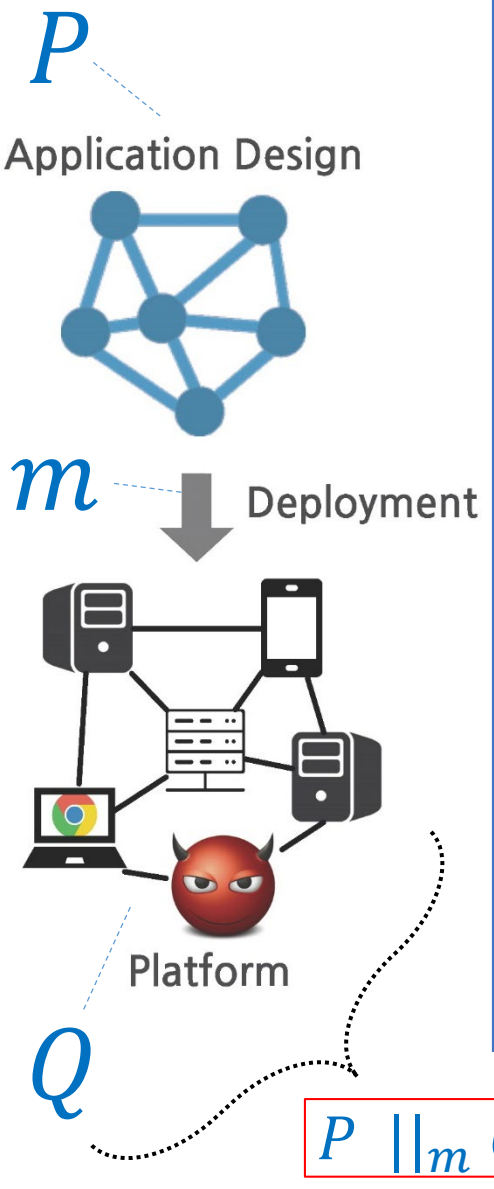
SaTC: CORE: Medium: Collaborative: Bridging the Gap between Protocol Design and Implementation through Automated Mapping

PIs: Tripakis, Nita-Rotaru (Northeastern), Jackson (MIT), Lafortune (Michigan), Kang (CMU)

Main challenge:
How to guarantee the correctness of a security protocol is preserved during implementation?

Our approach:
1. Modular formal modeling: separate application model ***P*** (e.g., Oauth) from execution platform model ***Q*** (e.g., HTTP)
2. Model implementation decisions as mapping ***m***
3. Synthesize secure mappings ***m*** automatically



Results:
1. Formal models of OAuth, HTTP, etc, in Alloy
2. Prototype mapping synthesis tool (employs counter-example guided synthesis)
3. Synthesized automatically secure mappings for OAuth 2.0 and 1.0
4. Synthesized mappings describe mitigations to well-known attacks (e.g., session swapping, covert redirect, session fixation)
5. Full results at CAV'19 paper