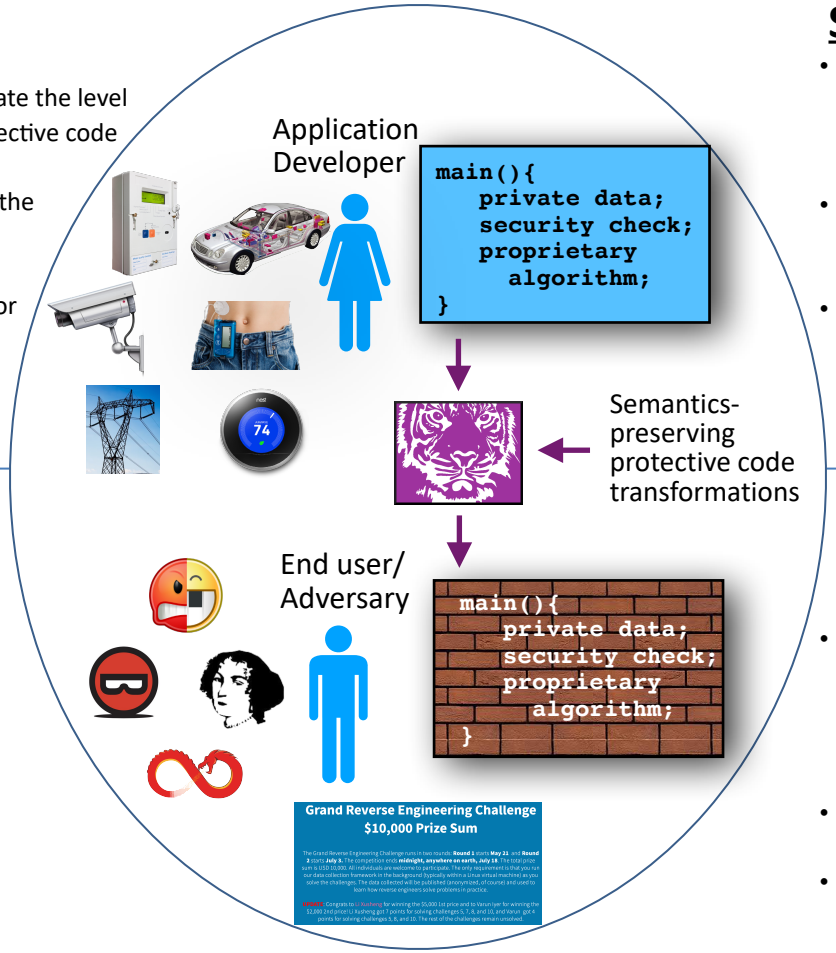
The Tigress Endpoint Protection Tool
Transition to Practice

Challenge:

- The security community lacks ways to evaluate the level of protection afforded by sequences of protective code transformations.
- A prerequisite for any evaluation strategy is the availability of a tool that can protect **real** programs with a comprehensive set of **state-of-the-art** transformations, for all major **platforms**.
- No such tool has been available.

Solution:

- We are building a freely available tool to aid developers of software protection tools as well as adversarial program analysis tools.
- We are building systems for collecting, analyzing, and visualizing data on reverse engineer behavior, collected through our *Grand Reverse Engineering Challenges*.



Scientific Impact:

- Academics use Tigress as an adversary to evaluate how novel program analysis/ malware detection algorithms fare against highly obfuscated code.
- Industry uses Tigress to experiment with software protection before investing in commercial tools.
- Strong endpoint protection is necessary to protect IoT devices against end-user attacks (extracting proprietary data including intellectual property and user credentials).

Broader Impact and Broader Participation:

- Attacks on endpoints by those who operate them are frequently ignored when doing security analysis, yet endpoints often form an easily penetrable part of the attack surface.
- Freely available endpoint protection tools is a step in solving this problem.
- Tigress has been used in Computer Security courses to generate reverse engineering assignments.

SaTC/TTP 2040206, University of Arizona,
Christian Collberg, collberg@cs.arizona.edu,
https://tigress.wtf, https://grand-re-challenge.org