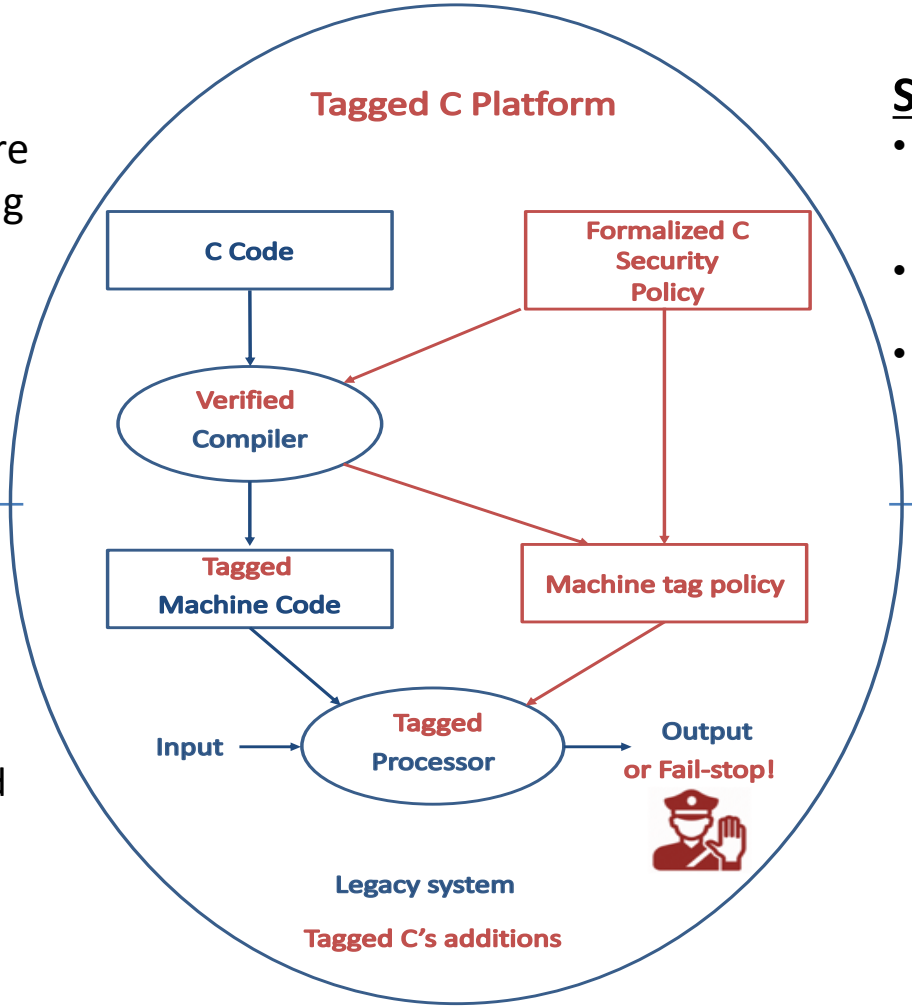
Specifying and Verifying Secure Compilation of C Code to Tagged Hardware

Portland State UNIVERSITY

Challenge:

Build a provably secure platform for executing legacy C code on hardware with tag-based monitoring



Scientific Impact:

- Makes hardware-based C security platforms more flexible and reliable
- Illuminates definition of C security properties
- Identifies fundamental requirements for verified compilation of C dialects

Solution:

- Formal specification of C security properties
- Formally verified compiler down to tagged hardware, based on novel C semantics

Broader Impact and Broader Participation:

- Mitigate security exploits based on legacy C insecurities
- Illustrate utility of formal methods to enhance security

NSF 2048499 PI: Andrew Tolmach, Dept. of Computer Science, Portland State University, tolmach@pdx.edu