TWC: Small: Empirical Evaluation of the Usability and Security Implications of Application Programming Interface Design

PIs: Brad A. Myers¹, Sam Weber², and Robert Seacord³

Contributing researchers: Michael Coblenz⁴, Whitney Nelson⁵, Jonathan Aldrich⁶, Joshua Sunshine⁶

Person

class is

immutable

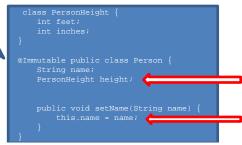
Carnegie Mellon University

¹Human Computer Interaction Institute, ²New York University, ³NCC Group, ⁴Computer Science Department, ⁵REU summer student, ⁶Institute for Software Research

Challenge:

Develop and empirically test concrete and actionable API and programming language design principles that lead to more secure code.

Glacier:



Scientific Impact:

- Cilk Plus's mechanism for defining reducers is more usable than OpenMP's, and has a more familiar syntax.
- Characterized many different ways to restrict changes, and identified that programmers needs are not met by today's systems.
- Created Glacier annotations for Java that enforce immutability.

Error: can't include mutable object in immutable class

Error: can't assign to field of immutable class

DSL for Blockchain programming will provide usable verification of key correctness properties, and reasoning about resource usage.

Users who made errors enforcing immutability (after all tasks) final Glacier 10/10 0/10

Solution:

- Evaluate usability of OpenMP and Cilk Plus proposed parallelism extensions to C and C++
- Understand and provide better immutability features
- Domain-specific language (DSL) for programming Blockchain programs

<u>Glacier</u>: Annotation system for Java which **statically** enforces **transitive** class **immutability**.

 User study showed works better than final: prevents real-world bugs and security vulnerabilities; usable with minimal training

Broader Impact:

- All programmers will better understand and write better security-relevant code.
- Show how designers can better take into account and test usability of programming and API features.

NSF CNS-1423054 9/1/2014 - 8/31/2017 Carnegie Mellon University