Toward Trustworthy Mutable Replay for Security Patches

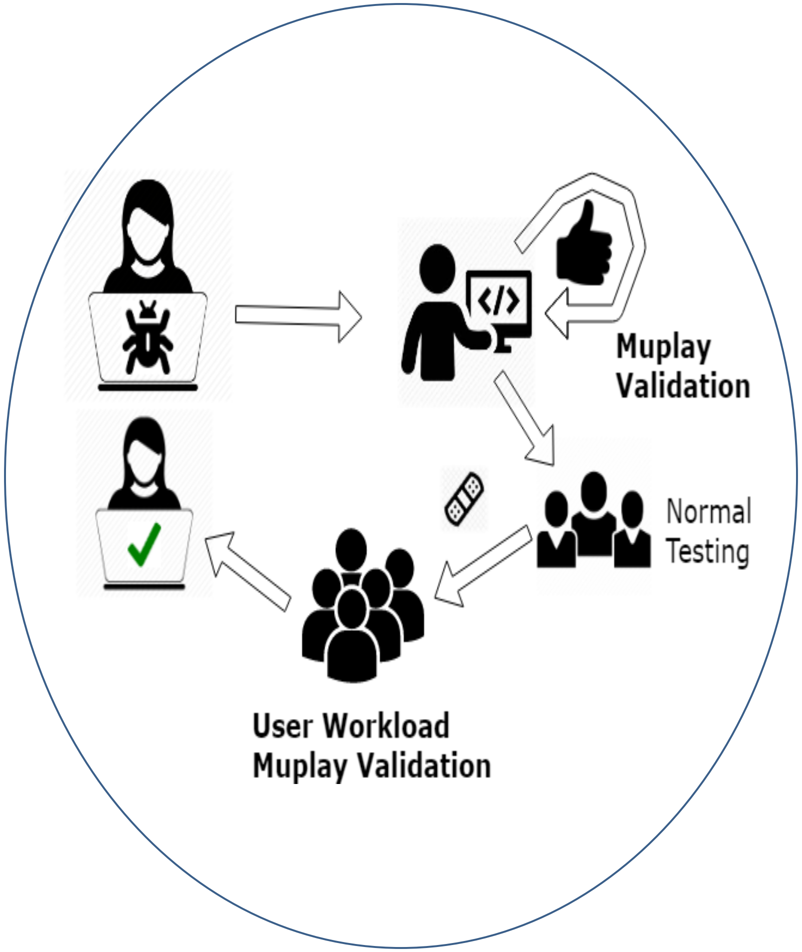
Challenge:

- Security vulnerability discovered in wild
- Need to rapidly generate tests for candidate patches when no existing developer test detects vulnerability
- We assume record-replay used to reproduce

Solution:

- Binary rewriting quilts modified function(s) into recorded executable
- Mutable replay (muplay) reuses stack, registers, memory to test candidate patch(es)
- Automatically mocks recorded environment during testing in developer environment
- Patch released with metadata for users to muplay their workloads with patched application

CNS-1563555, Columbia University,
Gail Kaiser and Jason Nieh
Contact: Kaiser@cs.columbia.edu



Scientific Impact:

- Difficult for developers to write tests that reproduce exact circumstances of security vulnerability and test candidate patches under those circumstances
- Muplay automatically generates tests for candidate patches, which conventional record-replay cannot do
- Test generation complements and does not replace normal regression testing

Broader Impact:

- Many security issues stem from failure to apply critical patches, because users afraid patches will break working functionality
- Now users can deploy patches with confidence
- Record-replay, test generation, fault localization, automated program repair, etc. topics in graduate course