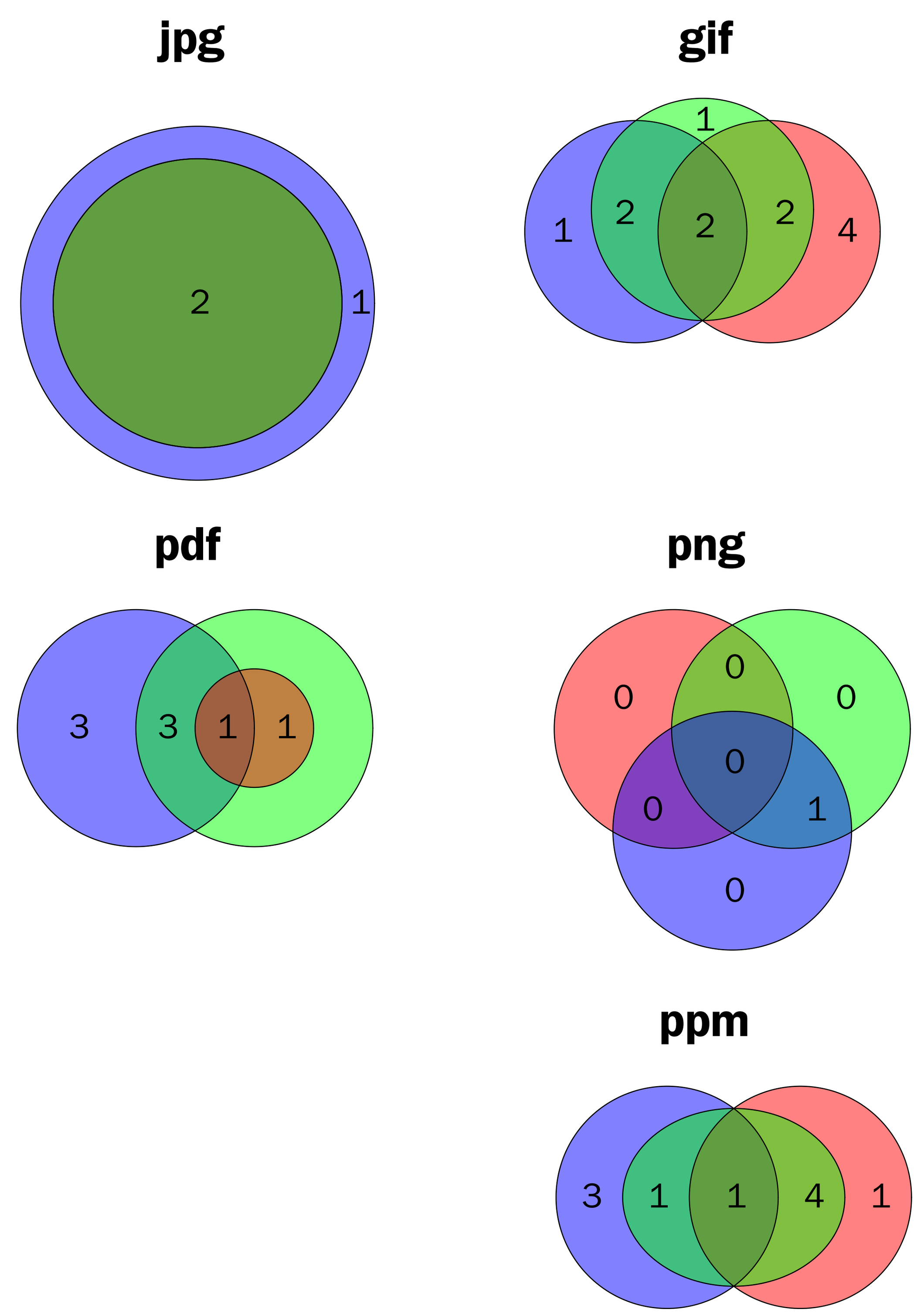
Vulnerability Discovery

Solving the vulnerability uniqueness problem

Current vulnerability discovery techniques such as black-box fuzz testing and concolic testing are so effective that they routinely find hundreds of thousands of crashers, which crash the target program. We created a new methodology for precisely and naturally defining vulnerabilities through the creation of patches. We use our methodology to study important questions regarding the practice of fuzzing.

Different seed files discover different vulnerabilities

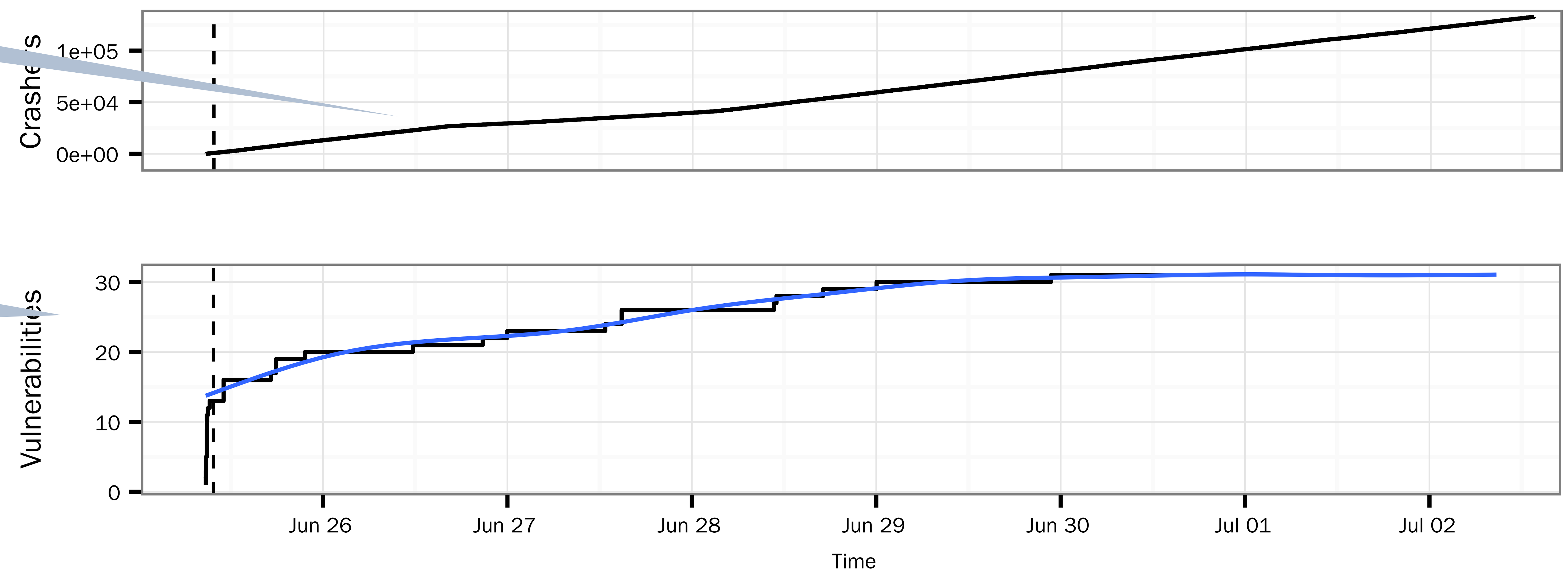


Experiment setup

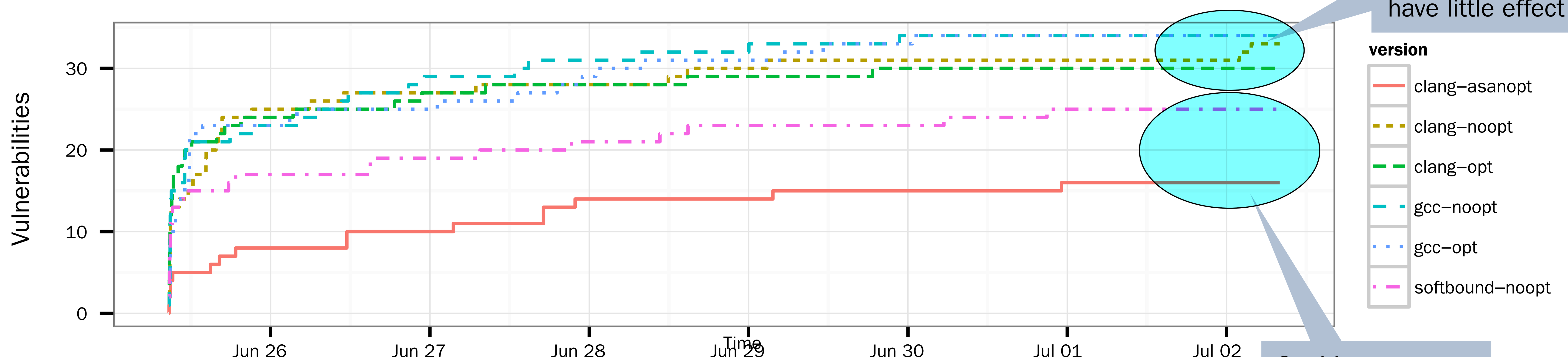
We fuzzed ImageMagick5.3.0 for a week under various configurations, which yielded over 130,000 crashes. We patched each crash using our methodology, which yielded 31 vulnerabilities. We used this data to answer:

Crash rate is constant

Vulnerability discovery rate slows down dramatically

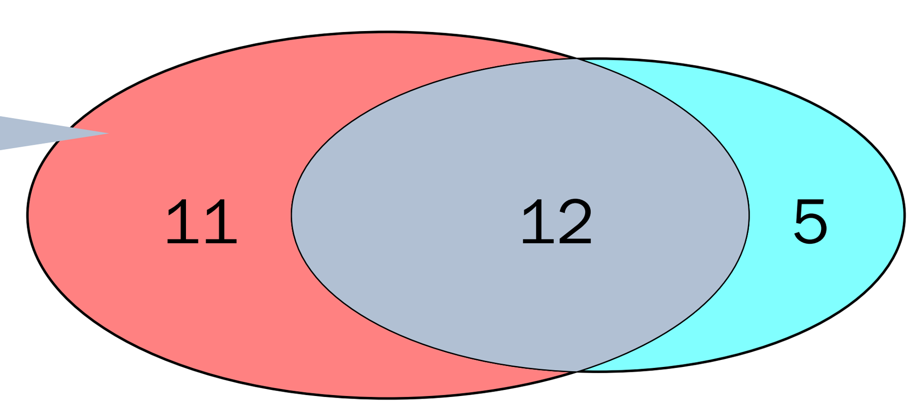


Compiler options have little effect



Sanitizers may not be worth their overhead

Different fuzzers find different vulnerabilities



Most crashes trigger multiple vulnerabilities

Vuls	1	2	3	4	5
Crashes	45859	79626	6860	21	1

Contact: Edward Schwartz eschwartz@cert.org

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0002859