BFF Release Notes

CERT Basic Fuzzing Framework (BFF) Significant changes

BFF 2.7 (September 23, 2013)

Virtual Machine changes

- Switch to Ubuntu from Debian

Code changes

- Use of PIN to uniquely identify crashes that trash the stack
- Optional feature to recycle crashing test cases as seed files
- Minimization to string defaults to Metasploit string

BFF 2.6 (October 19, 2012)

Code changes

- Incorporated CERT Triage Tools 1.04 to determine exploitability of crashes found.
- Integrated code improvements from FOE 2.0 release
- BFF 2.6 and FOE 2.0.1 use the same certfuzz package
- Improved fuzzing campaign recovery after VM reboot
- Detect and abort minimization if it takes too long (> 1hr)
- Fixed a bug in minimizer crash recycling
- Various bug fixes and improved error handling

BFF 2.5 (October 26, 2011)

Virtual Machine changes

- Upgraded to python 2.7
- Upgraded to gdb 7.2

Code changes

- BFF now runs on OSX in addition to Linux
- Support for multiple seed files
- Crashes found during minimization get analyzed as well
- Improved machine learning implementation applied to both seed file selection and rangefinder
- Improved crash uniqueness determination on Linux
- Minimizer tuned for performance
- callgrind generated on unique crashers for code coverage analysis
- default gdb output changed to provide additional details
- Basic crash clustering (analysis/callsim.py) using callgrind coverage analysis
- Optional minimization-to-string feature

BFF 2.0 (February 14, 2011)

Virtual Machine changes

- Added python libraries: Numpy, Scipy, Matplotlib

Code changes

- Ported BFF from Perl to Python
- Complete rewrite of crasher minimization using probability-based algorithm
- Added 'rangefinder' capability to automatically discover optimal fuzzing probability range(s)
- Restructured output directory (./crashers), now organized by crash hash
- Added analyzer scripts for visualization & fuzz run analysis

BFF 1.1 (September 21, 2010)

Virtual Machine changes

- Updated to Debian Squeeze for newer libraries.
- Installed generic vesa video driver for increased VM compatibility.
- Fixed strip symlink to /bin/true .

Code changes

- Forcibly kill gdb
- Removed unused tty information
- Updated to save SIGABRT crashes, discarding those caused by failed. asserts. Failed asserts can be saved through config option.
- Refactored perl script for increased performance and usability.
- Added crasher minimization script

BFF 1.0 (May 17, 2010)

- Initial Release