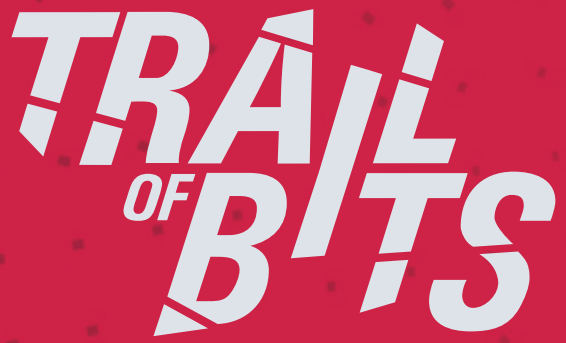


Static and Dynamic Analysis Tool Shootout

Interesting and Novel Binary Occultism Tradeshow

2016

Agenda

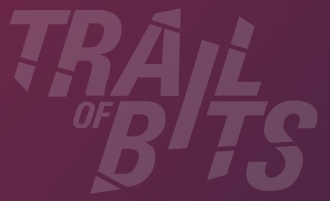
Introduction to Cyber Grand Challenge

The challenge sets

Porting status

Some analysis results

Cyber Grand Challenge




CYBER
GRAND CHALLENGE
DARPA
CYBER
DARPA
SECURE
MAYHEM
SCORING

Cyber Grand Challenge

DARPA created a “Grand Challenge” to improve automated software analysis.

By putting on a machine-on-machine CTF.

They spent millions creating the infrastructure:

- A custom OS ABI – DECREE
- Hundreds of challenge sets
- Testing Infrastructure

DECREE

A binfmt Linux ABI meant to reduce complexity.

Implements only 7 syscalls:

- exit, send, recv, mmap, munmap, select, getrandom
- These syscalls are neutered

No modern security mitigations (e.g. ASLR, NX Stack)

DARPA distributed Linux VMs that supported both ELF and DECREE

Challenge Sets

247 C & C++ network services

- Implementing things like mail servers, like ftp servers, etc
- Except all have custom protocols, no real RFCs allowed

All have 1 or more exploitable or crashing vulnerability.

You're expected to develop a "Proof of Vulnerability"

Challenge Sets (Continued)

Each challenge has:

- A detailed readme
  - Vulnerability Description
  - Vulnerability CWE
  - A “Challenges” section
- Polls (aka input generators) with high code coverage
- One or more Proof of Vulnerability triggers
- Included patches, guarded by compile-time #ifdefs

Example: Modern Family Tree

2527 lines of C
946 lines of Python (poll generator)

Description: In our society, family structures have changed such that traditional Family Tree software cannot properly model all current family structures. In response to this diverse environment, Family Relations Inc. brings to you our latest app, Modern Family Tree. It is the premier family tree building software for today's society.

Two vulnerabilities: 2x Heap Buffer overflows due to indexing 1 item too far

CWE-122 Heap-based Buffer Overflow
CWE-129 Improper Validation of Array Index
CWE-193 Off-by-one Error
CWE-788 Access of Memory Location After End of Buffer

Porting Status

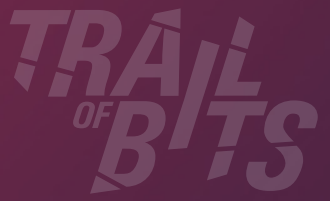
DECREE isn't all that useful

These challenges are a great test set so we decided to port them to Linux and OS X!

Porting Status:

- Rewrote the build system to be Cmake.
- Wrote C shim layers between decree ABI and posix
- Everything is dynamically linked now
- All build, almost all pass their polls
- Need to normalize it a bit more

The Shootout



Setup

Originally wanted to compare static analysis tools such as angr, pysymemu, klee, kite, cloud9.

And tools like clang-static-analyzer, coverity scan, pvs studio, etc.

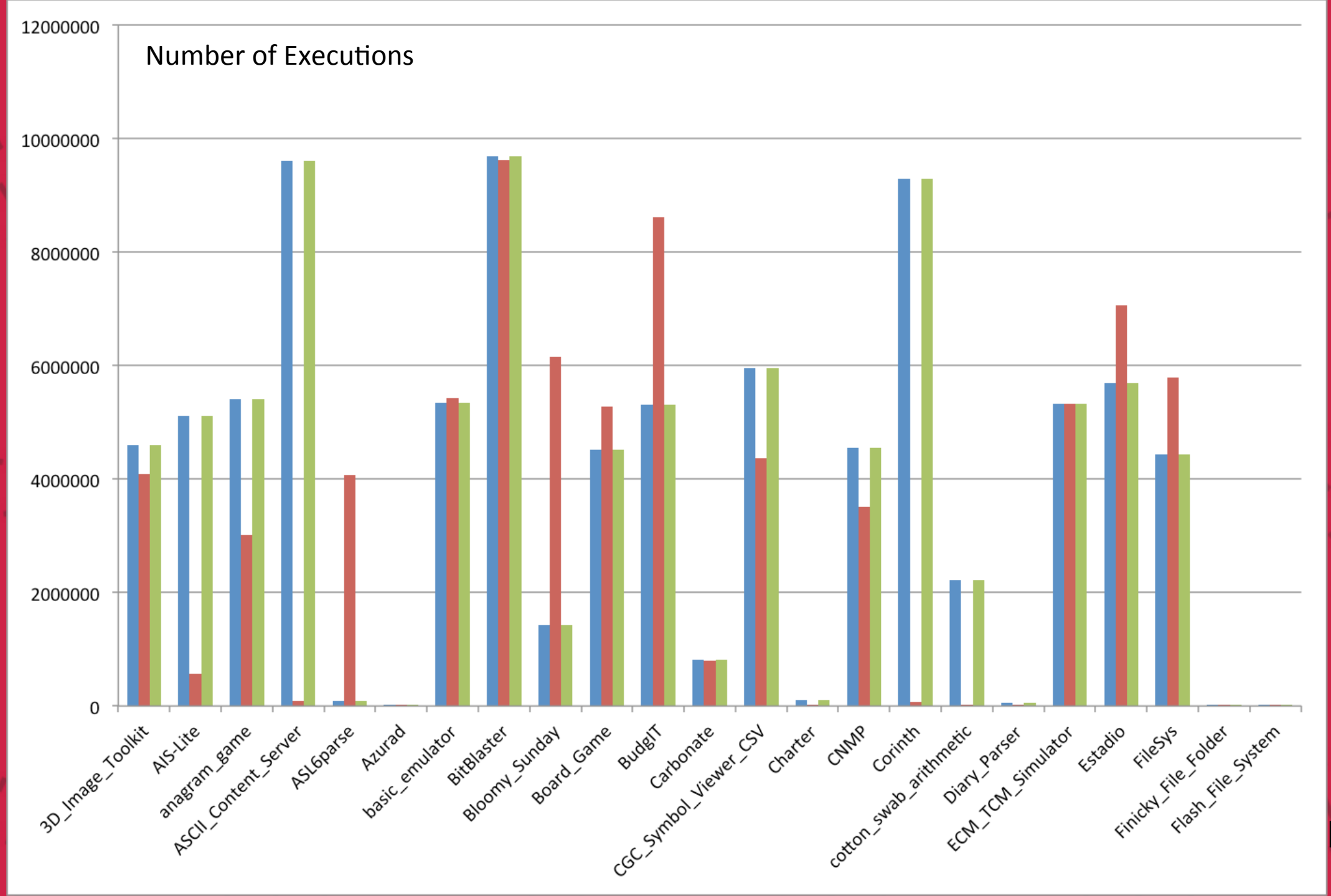
…but I ran out of time

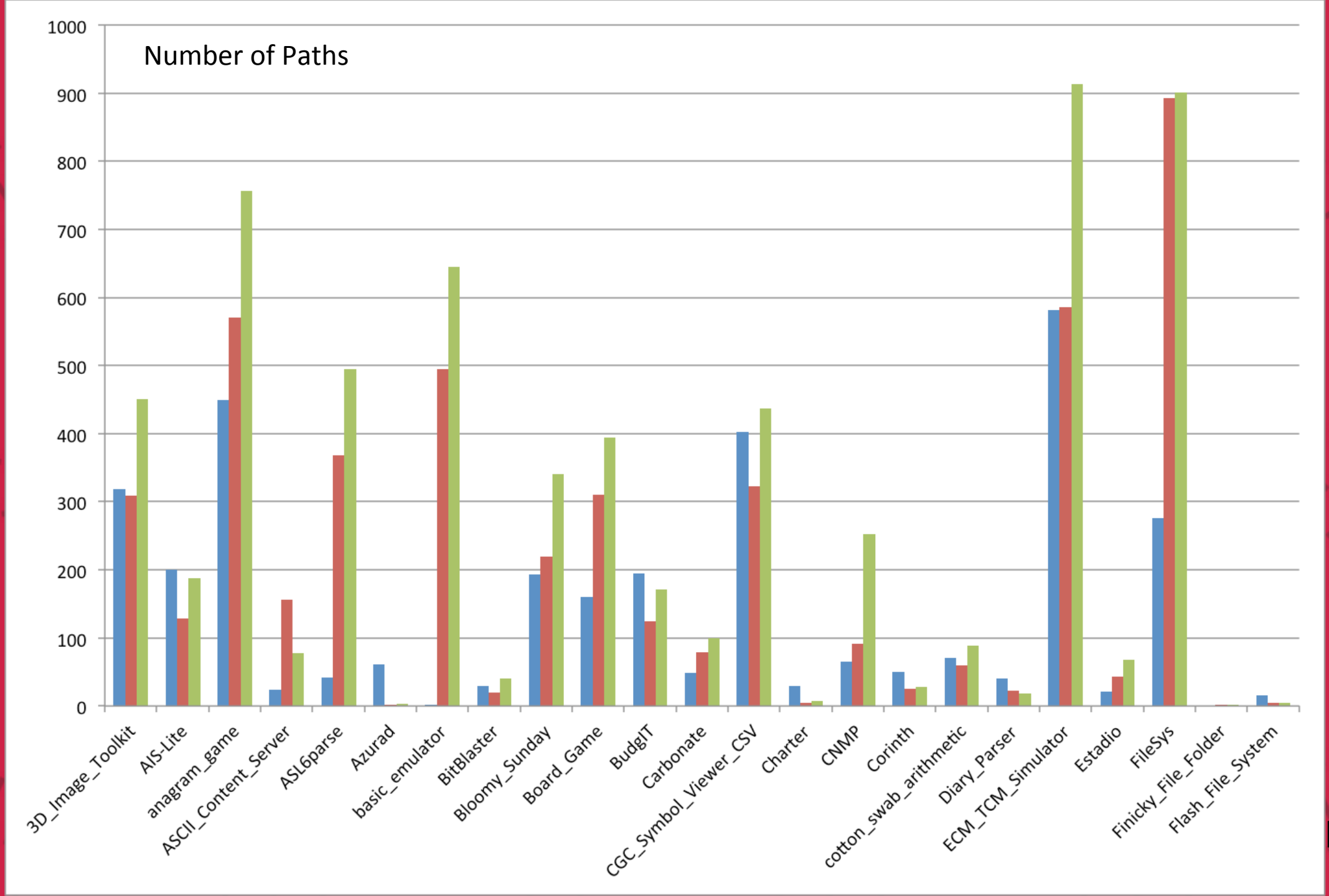
AFL vs. AFL vs. AFL (w/LAF)

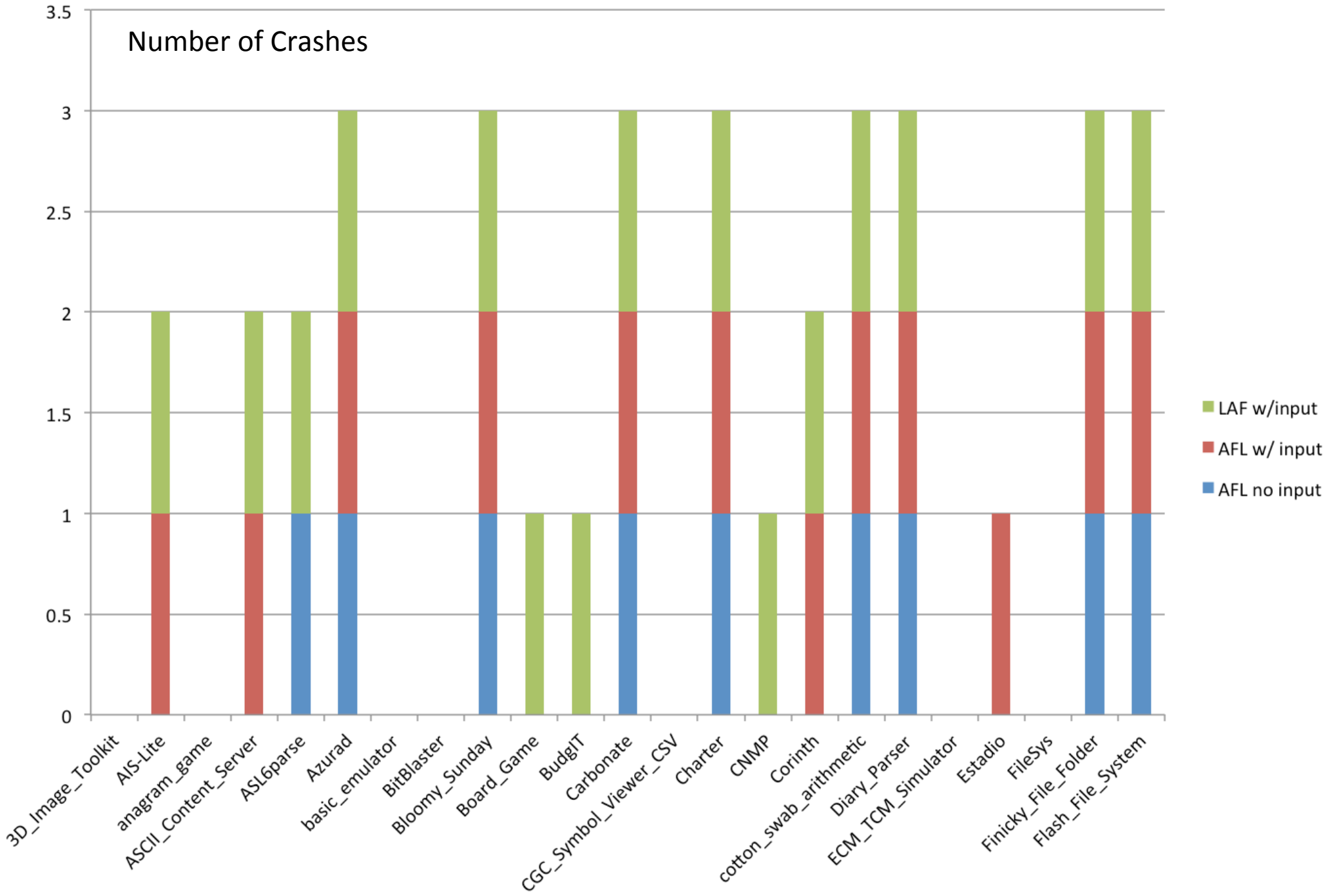
I took 23 binaries, 12 c3.xlarge ec2 instances, and 3 configurations of AFL.

- AFL with a single 4 byte input “eeee”
- AFL with 5 inputs ripped from the “transmit” side of the polls
- AFL + LAF* with 5 inputs

Each ran until the first crash or 10 hours. This turned out to be a mistake.


Number of Executions
12000000
10000000
8000000
6000000
4000000
2000000
0
3D_Image_Toolkit
AIS-Lite
anagram_game
ASCII_Content_Server
ASL6parse
Azurad
basic_emulator
BitBlaster
Bloomy_Sunday
Board_Game
BudgIT
Carbonate
CGC_Symbol_Viewer_CSV
Charter
CNMP
Corinth
cotton_swab_arithmetic
Diary_Parser
ECM_TCM_Simulator
Estadio
FileSys
Finicky_File_Folder
Flash_File_System


Number of Paths
1000
900
800
700
600
500
400
300
200
100
0
3D_Image_Toolkit
AIS-Lite
anagram_game
ASCII_Content_Server
ASL6parse
Azurad
basic_emulator
BitBlaster
Bloomy_Sunday
Board_Game
BudgIT
Carbonate
CGC_Symbol_Viewer_CSV
Charter
CNMP
Corinth
cotton_swab_arithmetic
Diary_Parser
ECM_TCM_Simulator
Estadio
FileSys
Finicky_File_Folder
Flash_File_System


Number of Crashes
3.5
3
2.5
2
1.5
1
0.5
0
3D_Image_Toolkit
AIS-Lite
anagram_game
ASCII_Content_Server
ASL6parse
Azurad
basic_emulator
BitBlaster
Bloomy_Sunday
Board_Game
BudgIT
Carbonate
CGC_Symbol_Viewer_CSV
Charter
CNMP
Corinth
cotton_swab_arithmetic
Diary_Parser
ECM_TCM_Simulator
Estadio
FileSys
Finicky_File_Folder
Flash_File_System
LAF w/input
AFL w/ input
AFL no input

Questions?

- Sorry about the lack of data. Expect a follow up blog post @ https://blog.trailofbits.com
- Challenge repository here: https://github.com/trailofbits/cb-multios
- Questions?

Ryan Stortz

Principal Security Researcher

ryan@trailofbits.com

@withzombies