FIG: Fault Injection in glibc

A Tool for Online Verification of Recovery Mechanisms

Pete Broadwell, Naveen Sastry and Jonathan Traupman

University of California, Berkeley

Objective/ Motivation

Objective:

- Develop a fault injection tool that can be run on a production system

Motivation:

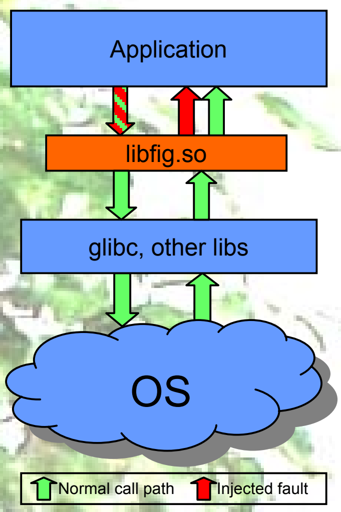
- Fault injection on a production system may expose latent faults
- Developers can benefit from advanced fault injection

Abstract

Enhanced software tools are necessary to evaluate the reliability and recoverability of applications under operating environment failures.

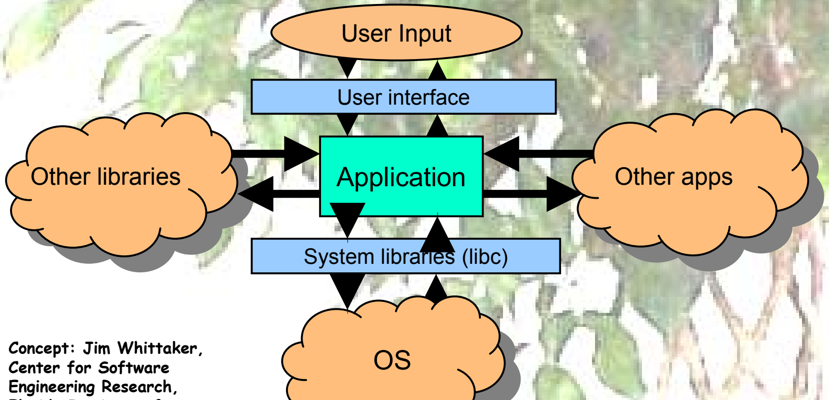
FIG is a lightweight, extensible software testing package that intercepts calls from applications to the operating system and injects errors to simulate system faults.

Implementation



- Thin stub library between application & other libraries
- Traps API calls
  - Logs them
  - Inserts faults
- Can be inserted into any application without modification
  - Uses LD_PRELOAD environment variable

"Software's Invisible Users"



Concept: Jim Whittaker, Center for Software Engineering Research, Florida Institute of Technology

Sample control file:

```
MALLOC_INDEX
  interval 82 to infinity
  return 0 errno ENOMEM
  probability 0.03


OPEN_INDEX
  // device out of space.
  interval 100 to infinity
  return -1 errno ENOSPC
  probability 0.001
  // kernel out of memory.
  interval 100 to 120 return -
  1 errno ENOMEM probability
  0.1
  // too many files open.
  callnumber 108 return -1
  errno EMFILE probability 1.0
```

Extensibility

- API stubs are auto-generated
- Very easy to add new APIs
- Control file specifies fault injection behavior

Conclusions

- Server apps are more robust than client apps
- Simple tricks help:
  - preallocation of resources
  - retries
  - graceful degradation
  - process pools

Test Results

Applications and Failure Types

	malloc()	read()	write()
Emacs, no X	crash	warning	warning
Emacs, w/X	crash	crash	crash
Apache	halts on preallocation	retries	no service
GNU File Utils	retry	retry	warning
MySQL Server	restart	Xact abort	Xact abort
Netscape	exit	exit	exit
Berkeley DB no Xacts	warning	warning	database corrupted
Berkeley DB w/Xacts	Xact abort	Xact abort	Xact abort
LPD	crash	exit	exit
zlib file compression	crash	warning	warning