RUMP KERNELS

ANYKERNELS

MEET

*FUZZING*

BY DR FUZZENSTEIN
WHO IS THIS GUY

BLOG @ AKAT1.PL
WORKS FOR LOGICALTRUST.NET
PENTESTER / BUG-HUNTER
EX-SOFTWARE DEVELOPER
OPEN SOURCE: PHP / NET / BSD / ...

FOUND BUGS IN VARIOUS PROJECTS:
IIS, APACHE, FREEBSD, NETBSD, DRAGONFLY BSD
OPENSCH, BINUTILS, ALPINE, STUNNEL ...

TWITTER: @AKAT1.PL
NetBSD

- BSD Licensed
- MultiArch
- Highly Portable
- 4.3BSD Derived
- It's Open and Free
- Kernel & Utilities
- Scalable
- Rump Kernels
- Great mature platform for your research

For more: www.netbsd.org
BSD & SECURITY

Are all BSDs created equally?

A survey of BSD kernel vulnerabilities

Very! Interesting talk...

...over 60 bugs in "net BSD"
Let's try to nail more bugs!

- ATF + Tests
- Security Team C
- MK Sanitizer
- KLEAK
- KASAN(4)
- KUBSAN(4)

NetBSD

- Quality Improvement Efforts
- Fuzzing
- Syzkaller
- AFL-TRIPFORCE

Rump to catch more bugs...
WHAT'S THE LOGO?

?? ?? ?? ?? ?? ?? ?? ??

NetBSD
LET'S PRETEND IT'S THE NETBSD KERNEL

NetBSD
RUMP STANDS FOR:

- Runnable
- User
- Meta
- Programs

WUT???
THE NET BSD KERNEL

ANY KERNEL

RUHP KERNEL RUNNING ON TOP OF LINUX

BT

VFS

INET

INET6

VFS

DRIVERS

802.11

INET

INET6
"CONTAINER"

FS
VFS
INET

APPLICATION

RUMP
RUMP USER

YOU CAN THINK IT'S A VERY LIGHT VM

IT CAN BE RUN ON TOP OF ANYTHING

INNER SPACE

USER SPACE

KERNEL SPACE

KERNEL

BARE METAL
WHY RUMP IS COOL?

1. WE CAN RUN TCP/IP STACK IN USERSPACE FS (SECURITY!) (SOLO, HUBO, ...)

2. WE CAN DEBUG PARTS OF THE KERNEL IN THE USERSPACE (YES! USING GDB)

3. WE CAN SPEED UP KERNEL DEV PROCESS
   NO NEED TO REBOOT, FANCY DEBUG SETUP, VMS ...

4. WE CAN USE USERLAND TOOLS GDB, SANITIZERS, GLUU, MODERN FUZZERS
DEMO

DDB vs GDB

+ RUMP

PING

RUMP CTRL SH

TCP: CONNFCTION

RUMP ALLSERVER

GDB

BREAK

ICMP INPUT
DARK & STORMY NIGHT IN THE FALL OF 1988

PROF. BARTON MILLER'S HOUSE

CMD ABC

\[ \text{NOISE} \]

CMD A & # ^ B \_ C C

CRASH

PHONE LINE

UNIVERSITY OF WISCONSIN-MADISON

FUZZING?
FUZZING FLAVOURS

CREATE RANDOM DATA AND SEE WHAT HAPPENS.  
DUMB FUZZING  
MONKEY TESTING

CREATE RANDOM DATA BASED ON FEEDBACK FROM PREVIOUS EXECUTIONS AND SEE WHAT HAPPENS  
FEEDBACK DRIVEN FUZZING

IF SMTH KNOT THEORY SOME PEOPLE CALL IT SMART FUZZING IS INVOLVED

AT LEAST THIS GUY IS NOT A NOOB
FUZZ RUMP . SH

FO RK OF BUILD RUMP . SH THAT LET YOU FUZZ THINGS

☑️ M . x → 9 . x

☑️ SANITIZER SUPPORT

☑️ CLANG / GCC

☑️ AFL SUPPORT (INCLUDING AFL-CLANG-FAST)

HTTPS://GITHUB.COM/ AKAT1 /FUZZ RUMP . SH/

./build rump . sh checkout git

./build rump . sh tools build install

TESTED ON UBUNTU 16.04 LTS
INTEGRATION WITH ADDRESS SANITIZER

MEMORY ALLOCATORS

- A HUGE ALLOC

POOL

VS

n SMALL ONES

POOL(3), MALLOC, KMEM(9), ...

NAME SPACE

APP

MEMSET

MEMSET

RUMP

RUMPNS_MEMSET

MEMSET

RUMPNS_MEMSET

ASAN CAN'T SEE IT

ASAN IS HAPPY!

LD_PRELOAD = .../interceptor.so

AFL INTEGRATION TALE
WHAT TO LOOK FOR?

* Memory Corruption
* Panics
* Leaks!
* Hangs
* Show Must Go On in case of the kernel

Why?

> Leak triggered from the remote is dangerous.
DUMB USE CASE - MINÉRVA-LIB

SYSCALL FUZZING USING RANDOM VALUES

MINÉRVA <-> TCP <-> RUMP ALL SERVER

DEMO!

DUMB FUZZER IS DUMB
RUMP FUZZ - FILESYSTEMS

Approach: Mount FS → Do some operations → Unmount

Tested EXT2, FFS and found dozen of crashes
RUMP Fuzz - Network

1. Approach #1: inject packets using raw socket problem. From client, there is no way to know if packet was handled.

2. Approach #2: expose input functions and inject packets directly.

Demo

Speed: 1Mok/s using persistent AFL mode

Problems:
- Checksums, stateful protocols, mbufs, not stable...
- Bugs found...
ZERO

ничего

UMGANGSSPRACHLICH

RIC

 налог
Yet

- Corpus can be reused as a test suite
  - Not a big surprise.
    - We need to dig deeper
    - Improve coverage
    - Cover more bug types
    - Tested well in the wild

At least we are not noobs...
FUTURE DIRECTIONS

- COVER MORE DRIVERS
  - 802.11
  - BLEUETOOTH
- OSS-FUZZ INTEGRATION
- IMPROVE COVERAGE
- OTHER OSes? LibOS?

... MORE

WE NEED YOU!
THANKS:

POOKA - ANTI KANTEE

MICHAL DARDAS & LOGICAL TRUST

#NETBSD-QA C FREE NODE

ETERNAL

RYOSHU - KAMIL RYTAROWSKI

MRG

THE NETBSD DEVELOPERS

DRAGONFLY TEAM

❤️
DISCUSSION

Q&A

FELL FREE TO CONTACT ME

SHM @ NetBSD.org

M.KOCIELESKI @ LOGICALTRUST.NET

#netbsd-qa @ FREENODE

shm @ FREENODE