RUMPKERNELS

~~ANYKERNELS~~

MEET

☆ FUZZING ☆

BY DR FUZZENSTEIN

@akat1_pl

WHO THE HELL IS THIS GUY

BLOG @ AKAT1.PL

WORKS FOR LOGICALTRUST.NET

PENTESTER \ BUGHUNTER

EX-SOFTWARE DEVELOPER

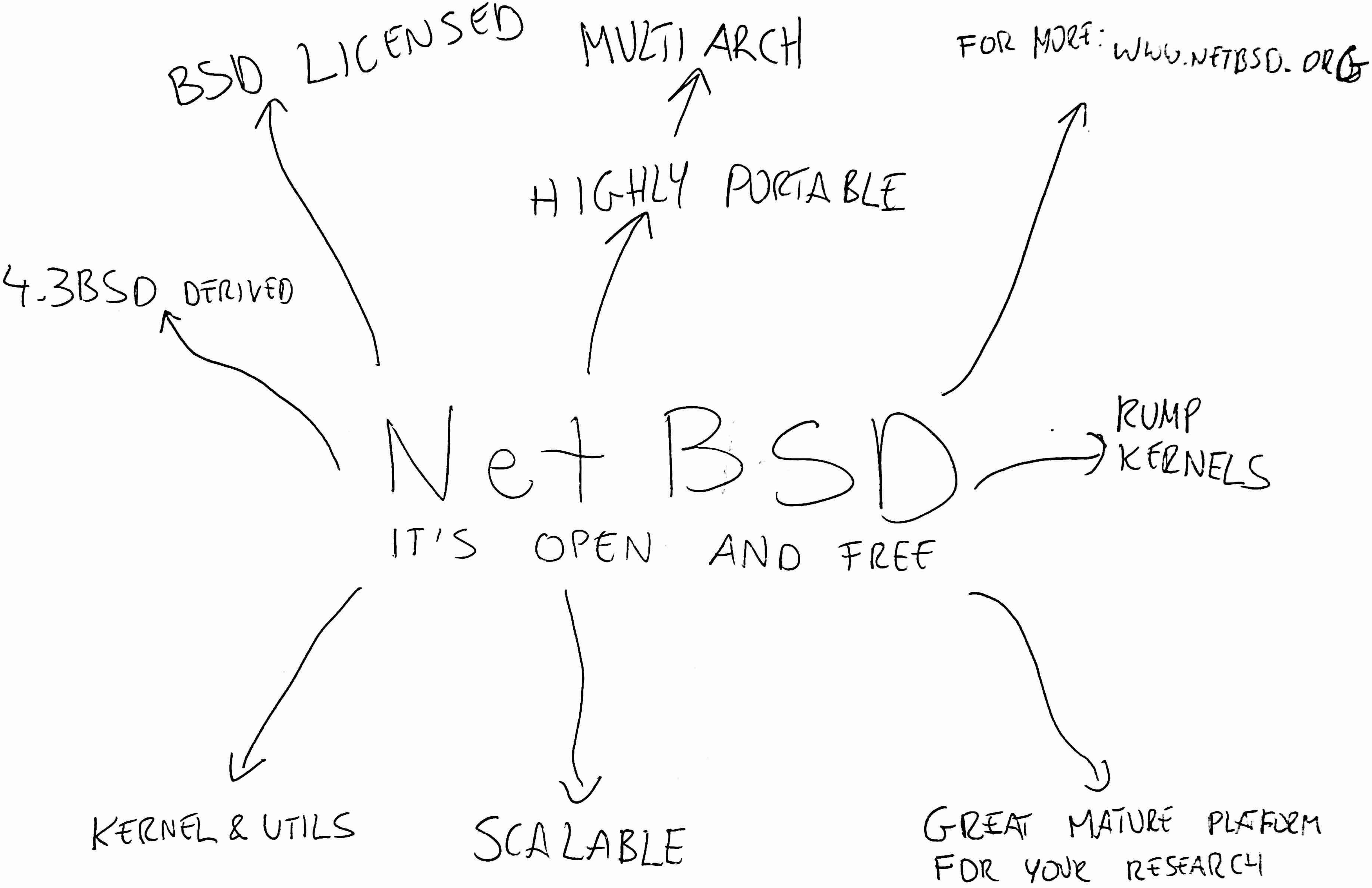
OPEN SOURCE: PHP / NETBSD / ...

FOUND BUGS IN VARIOUS PROJECTS:

IIS, APACHE, FREEBSD, NetBSD, DRAGONFLY BSD

OPENSSH, BINUTILS, ALPINE, STUNNEL ...

TWITTER: @akat1_pl



NetBSD

IT'S OPEN AND FREE

BSD LICENSED

MULTI ARCH

HIGHLY PORTABLE

FOR MORE: WWW.NETBSD.ORG

4.3BSD DERIVED

RUMP KERNELS

KERNEL & UTILS

SCALABLE

GREAT MATURE PLATFORM
FOR YOUR RESEARCH

BSD & SECURITY

ARE ALL BSDs CREATED EQUALLY?

A SURVEY OF BSD KERNEL VULNERABILITIES

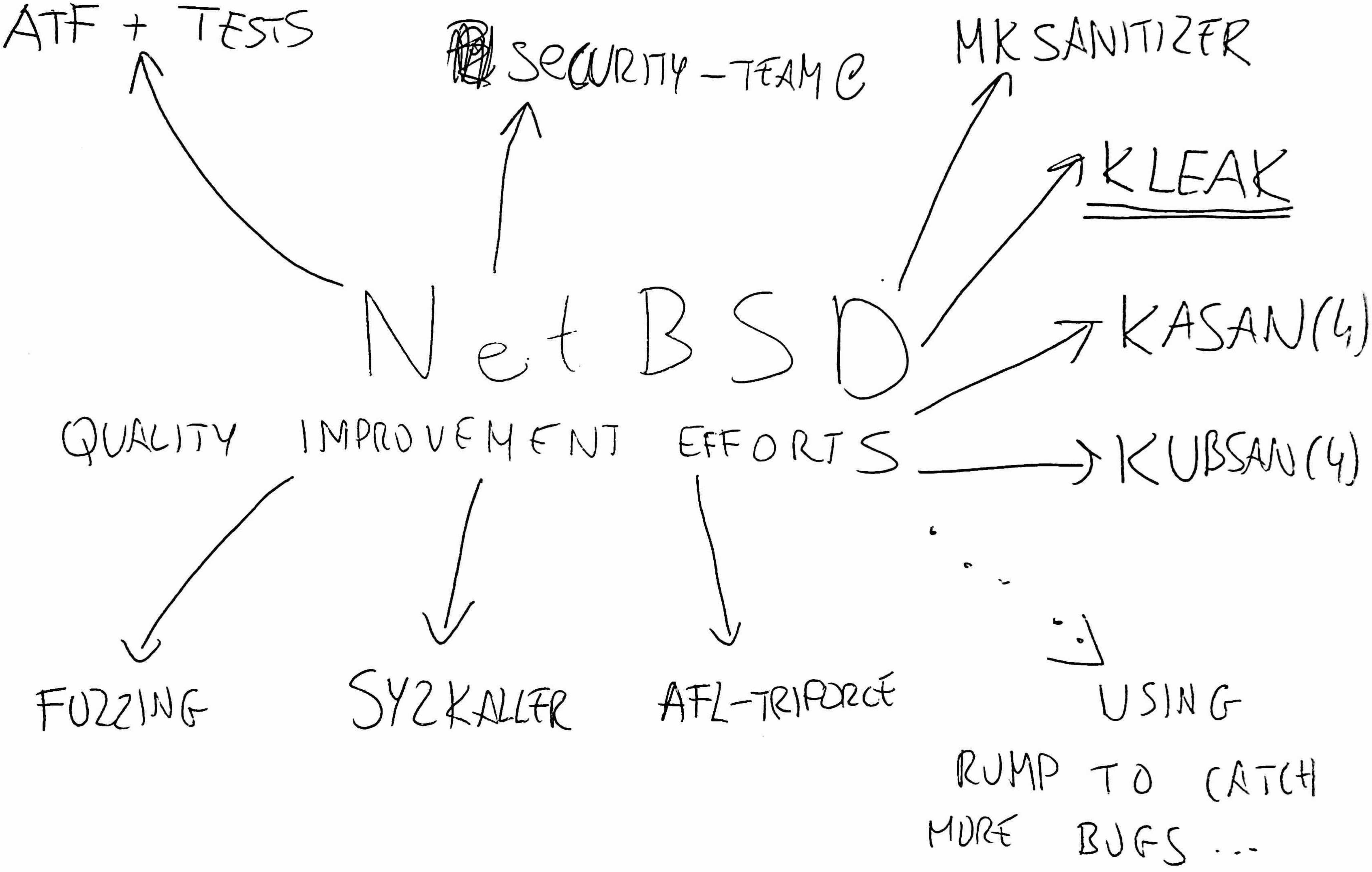
ILJA VAN SPRUNDEL

SORRY ILJA / TRIED MY BEST TO DRAW YOU!

VERY! INTERESTING TALK ☺

... OVER 60 BUGS IN THE NET BSD ☹

LET'S TRY TO NAIL MORE BUGS!



NetBSD

QUALITY IMPROVEMENT EFFORTS

ATF + TESTS

security-team@

MKSANITIZER

KLEAK

KASAN(4)

KUBSAN(4)

FUZZING

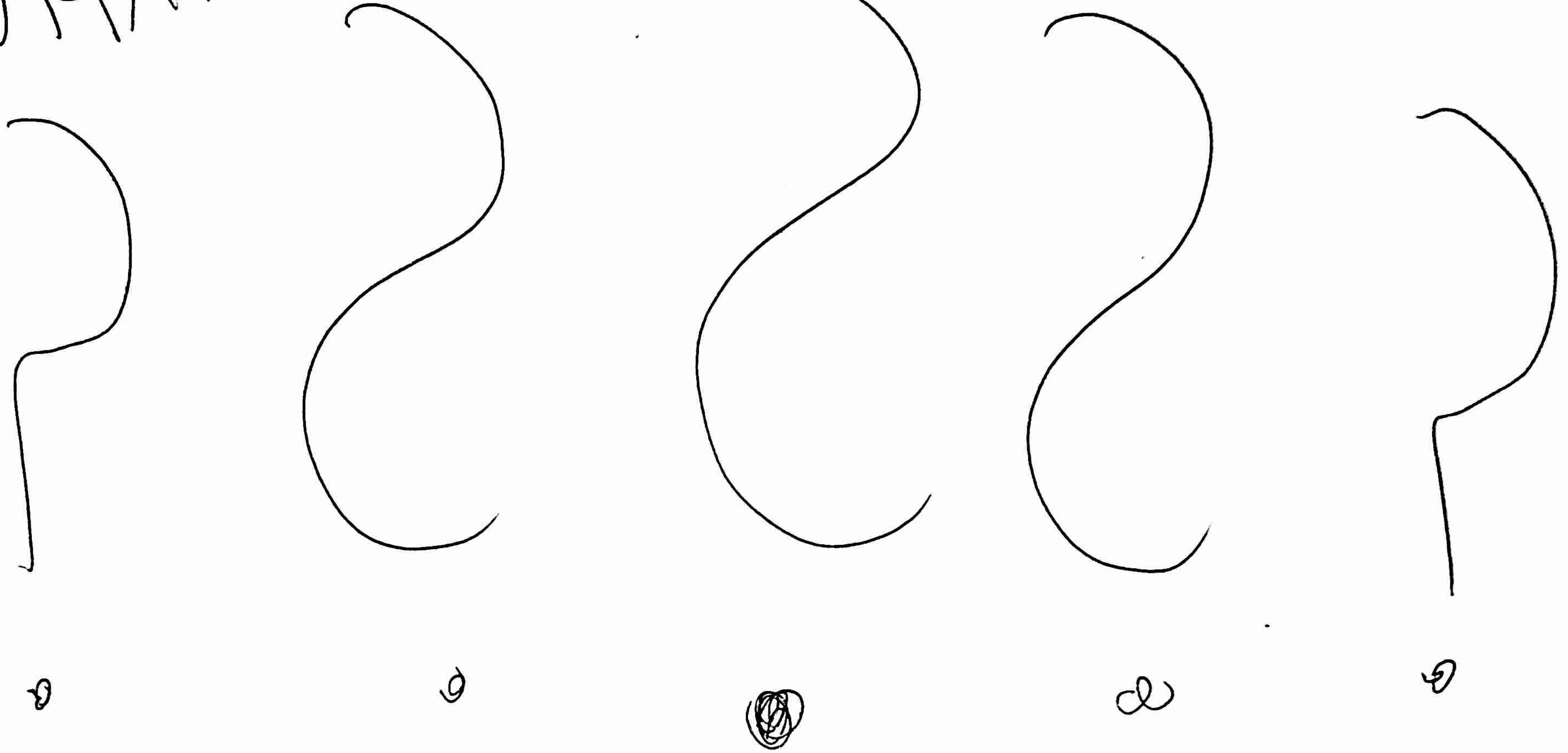
SYZKALLER

AFL-TRIFORCE

:)

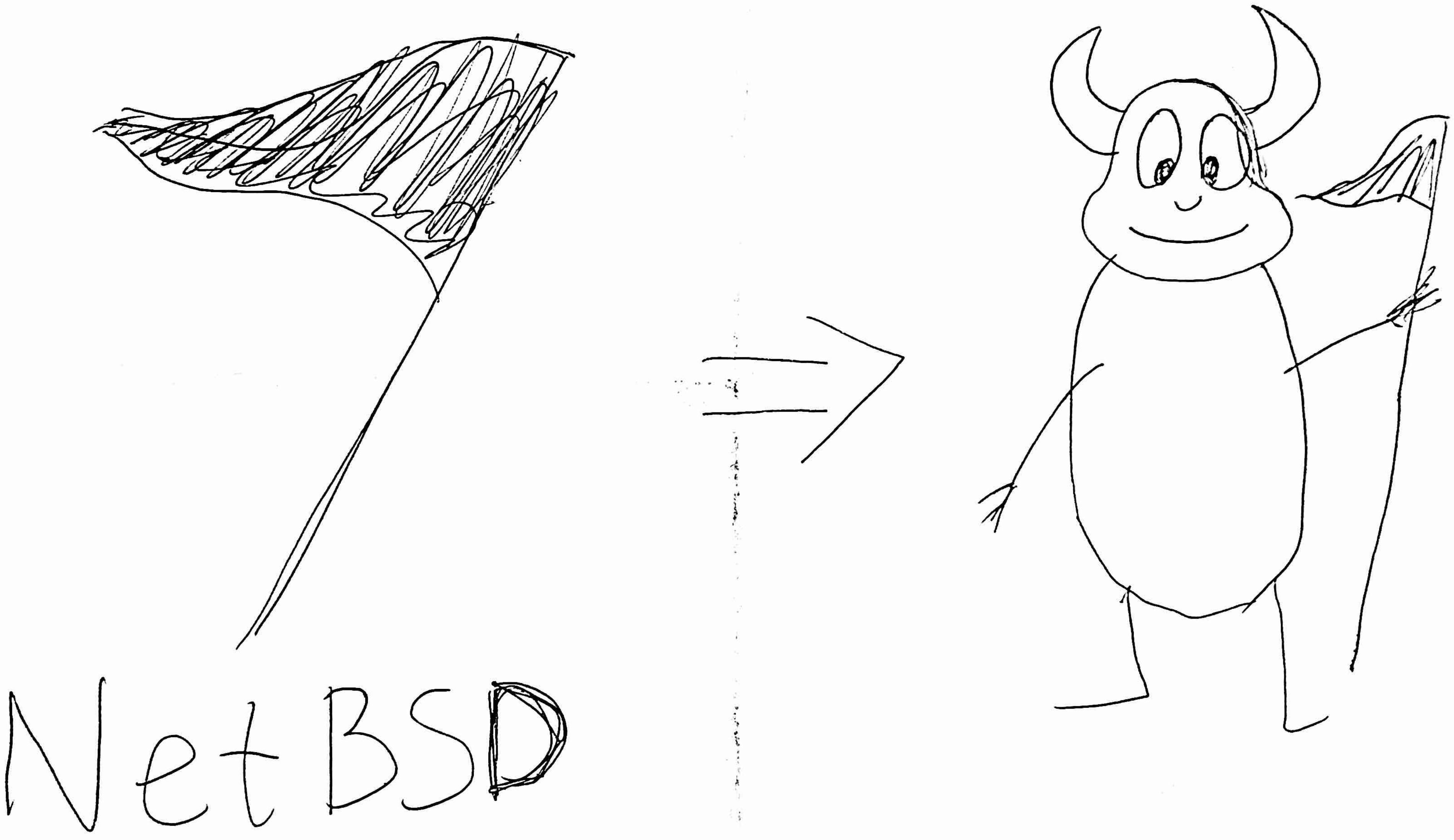
USING RUMP TO CATCH MORE BUGS ...

WHAT'S THE LOGO?



NetBSD

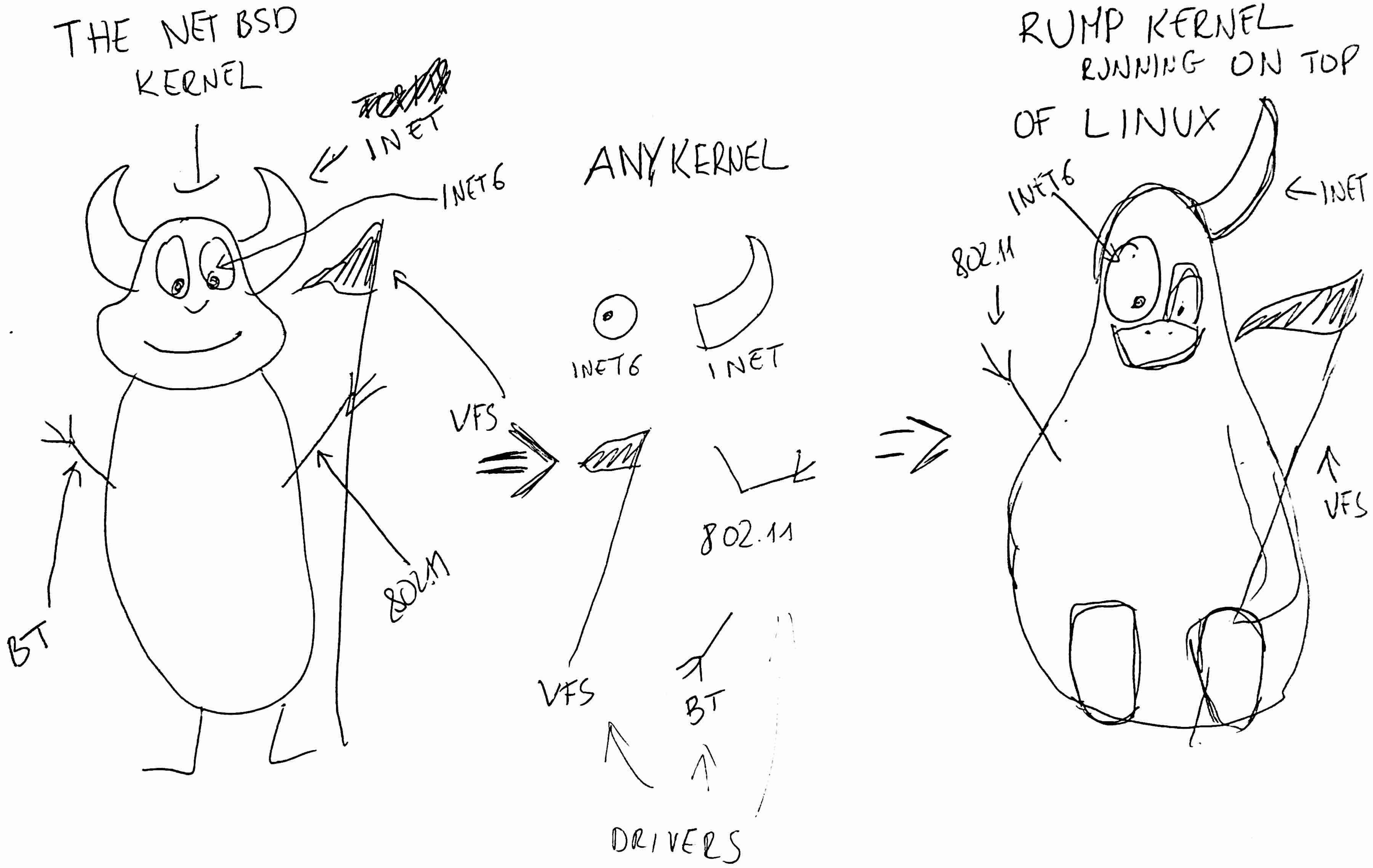
LET'S PRETEND IT'S THE NET BSD KERNEL

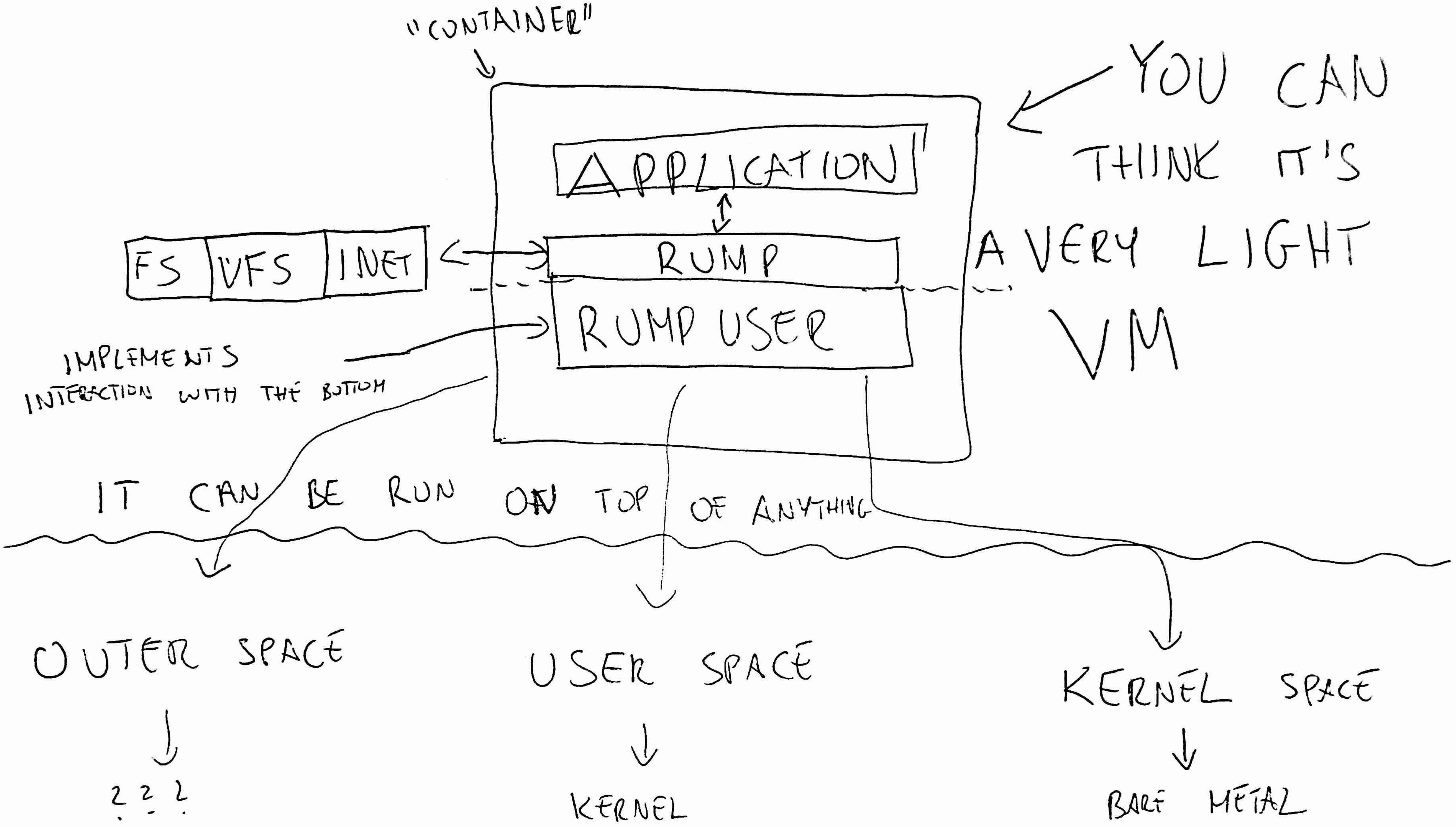


RUMP STANDS FOR:

RUNNABLE USER META PROGRAMS

WUT?


THE NET BSD KERNEL
INET
INET6
VFS
802.11
BT
ANYKERNEL
INET6
INET
802.11
VFS
BT
DRIVERS
RUMP KERNEL RUNNING ON TOP OF LINUX
INET6
INET
802.11
VFS



YOU CAN THINK IT'S A VERY LIGHT VM

IT CAN BE RUN ON TOP OF ANYTHING

WHY RUMP IS COOL?

BEST PRICE!!!

① WE CAN RUN TCP/IP STACK IN USERSPACE
FS

(SECURITY!) (SEL4, HURD, ...)

DEMO

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

DEMO

GDB VS DDB

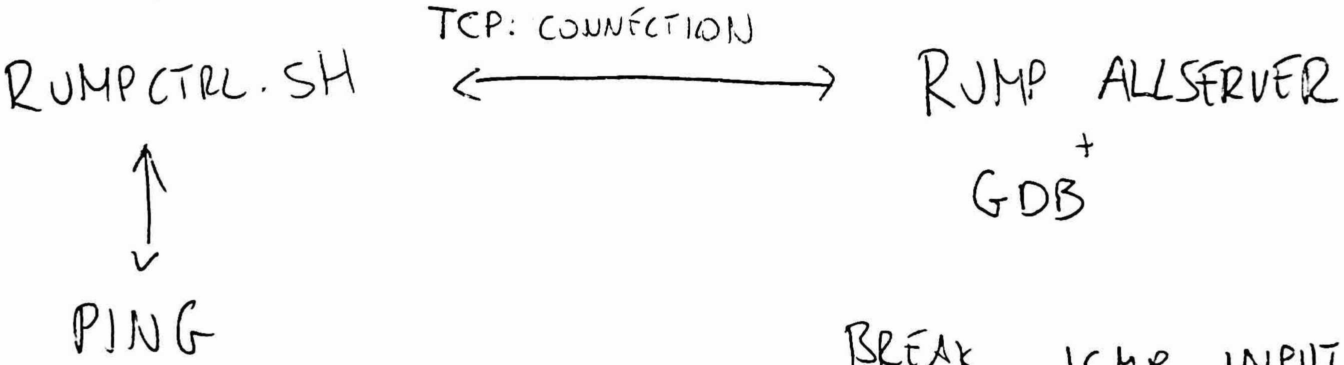
③ WE CAN SPEEDUP KERNEL DEV PROCESS
NO NEED TO REBOOT, FANCY DEBUG SETUP, VMS ...

④ WE CAN USE USERLAND TOOLS GDB, SANITIZERS, GCOV, MODERN FUZZERS

DEMO

DDB VS GDB

+RUMP



TCP: CONNECTION

RUMPCTRL.SH

RUMP ALLSERVER

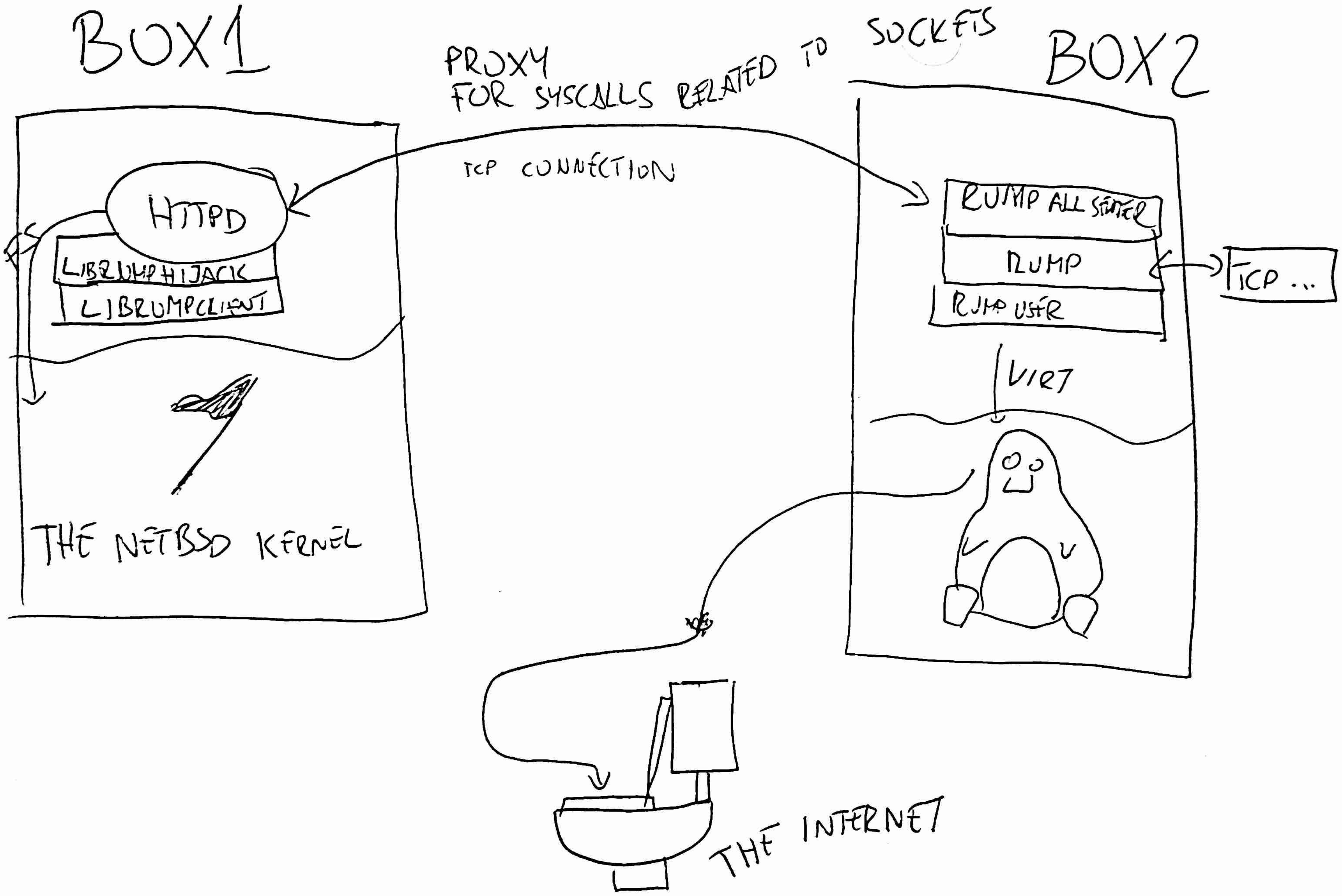
+

GDB

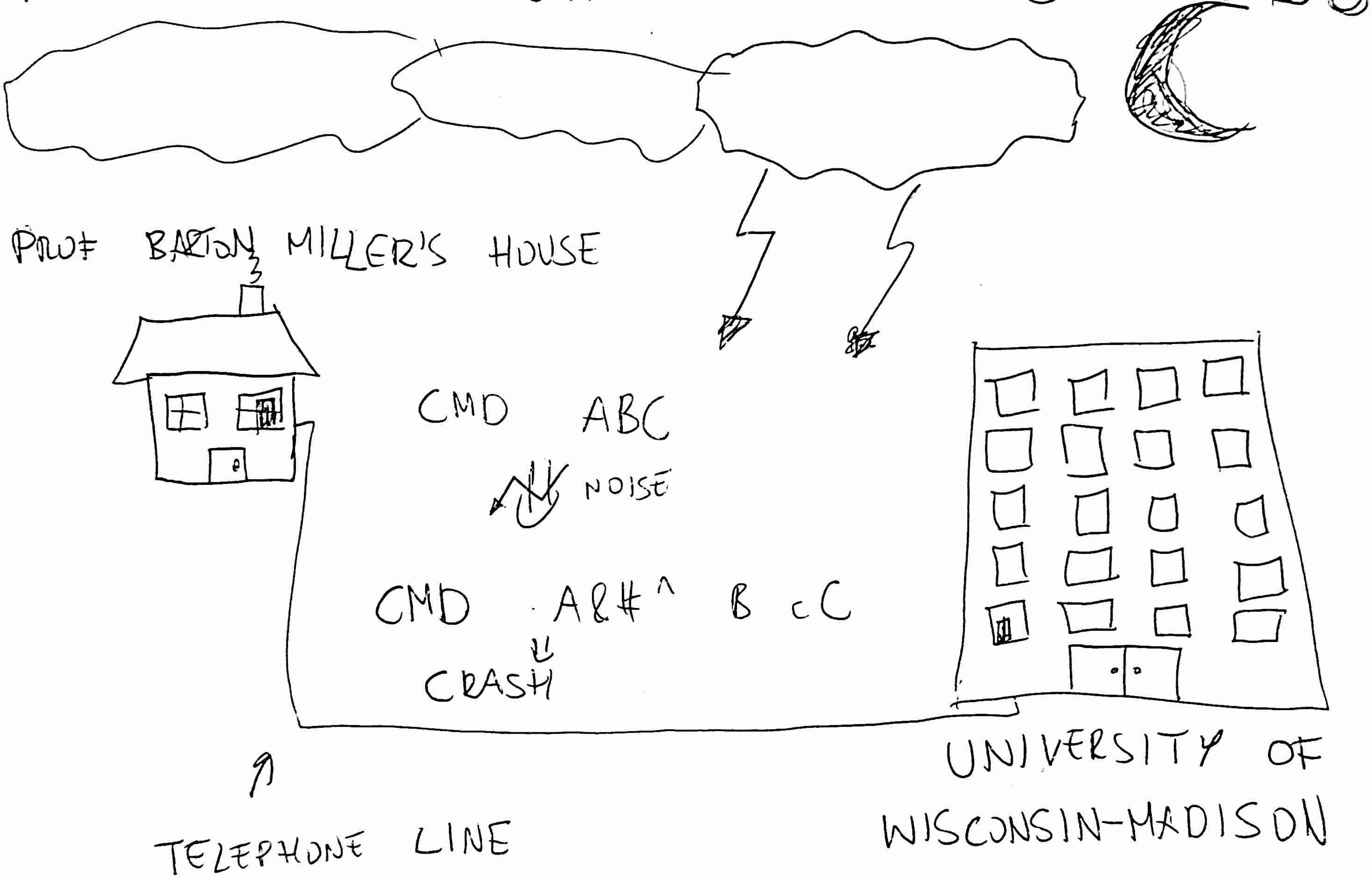
PING

BREAK ICMP_INPUT

DEMO


BOX1
BOX2
PROXY
FOR SYSCALLS RELATED TO SOCKETS
TCP CONNECTION
HTTPD
LIBRUMPHIJACK
LIBRUMPCLIENT
PS
THE NETBSD KERNEL
RUMP ALL SERVER
RUMP
RUMP USER
TCP ...
VIRT
THE INTERNET

DARK & STORMY NIGHT IN THE FALL OF 1988



FUZZING?

FUZZING FLAVOURS

CREATE RANDOM DATA AND SEE WHAT HAPPENS.

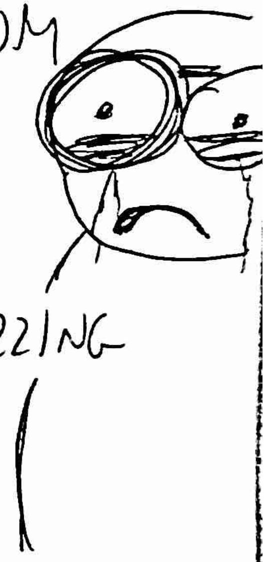
↖ DUMB FUZZING

MONKEY TESTING

CREATE RANDOM DATA BASING ON FEEDBACK FROM PREVIOUS EXECUTIONS AND SEE WHAT HAPPENS

^ FEEDBACK DRIVEN FUZZING

IF SMT /KNOT THEORY IS INVOLVED SUME PEOPLE CALL IT SMART FUZZING



AT LEAST THIS GUY IS NOT A NOOB →

FUZZRUMP.SH

FORK OF BUILDRUMP.SH THAT LET YOU FUZZ THINGS

- ✓ 7.x → 9.x
- ✓ SANITIZER SUPPORT
- ✓ CLANG / GCC
- ✓ AFL SUPPORT (INCLUDING AFL-CLANG-FAST)

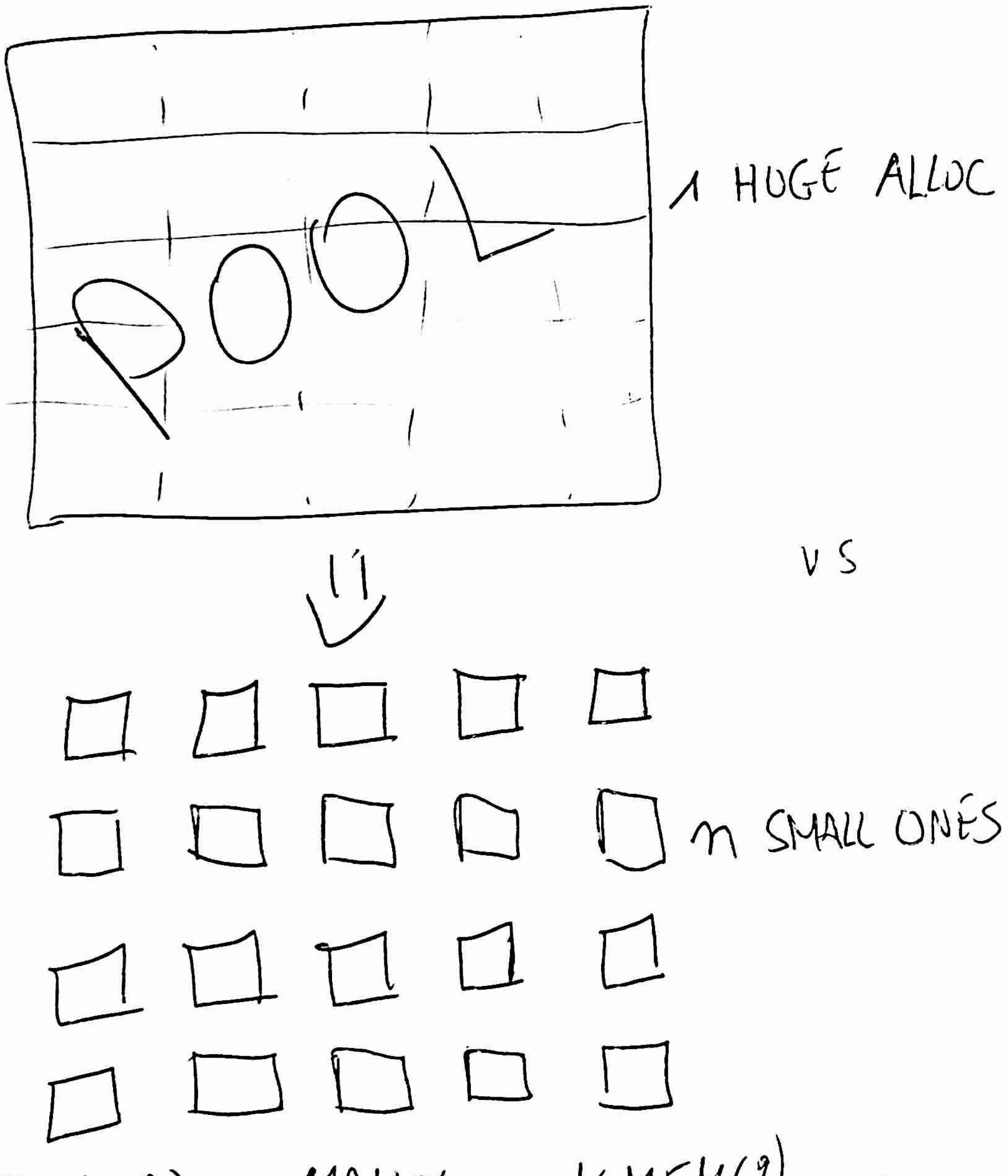
HTTPS://GITHUB.COM/~~FUZZRUMP.SH~~ AKAT1 / FUZZRUMP.SH/

```
./buildrump.sh checkout git
./buildrump.sh tools build install
```

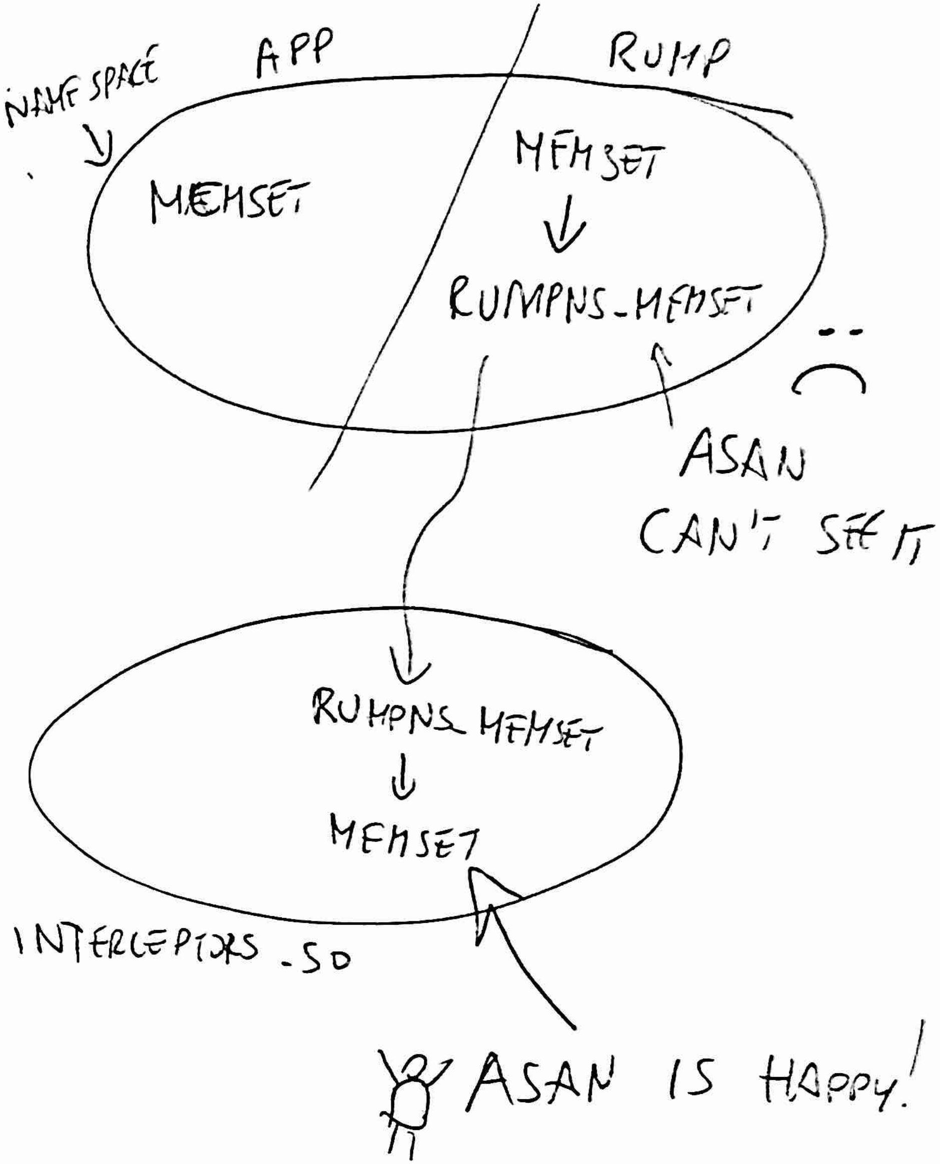
TESTED ON UBUNTU 16LTS

INTEGRATION WITH ADDRESS SANITIZER

MEMORY ALLOCATORS



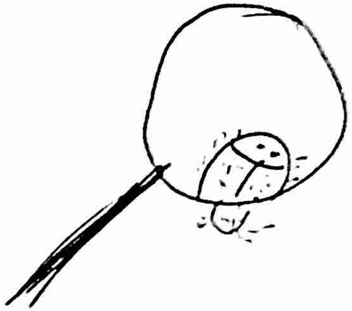
POOL(9), MALLOC, KMEM(9) ...



LD_PRELOAD=.../interceptor.so

AFL INTEGRATION TALE

WHAT TO LOOK FOR?



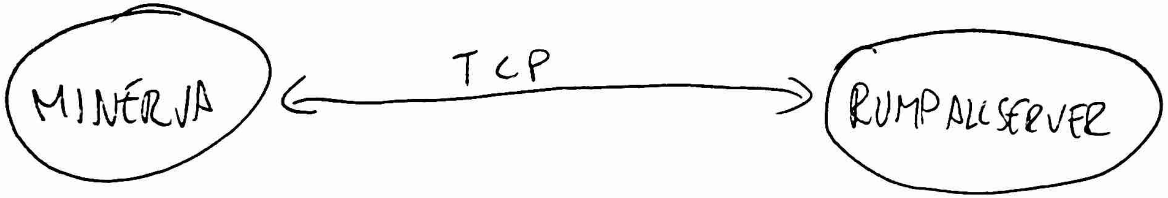
- MEMORY CORRUPTION
- PANICS
- LEAKS!
- HANGS
- SHOW MUST GO ON IN CASE OF THE KERNEL

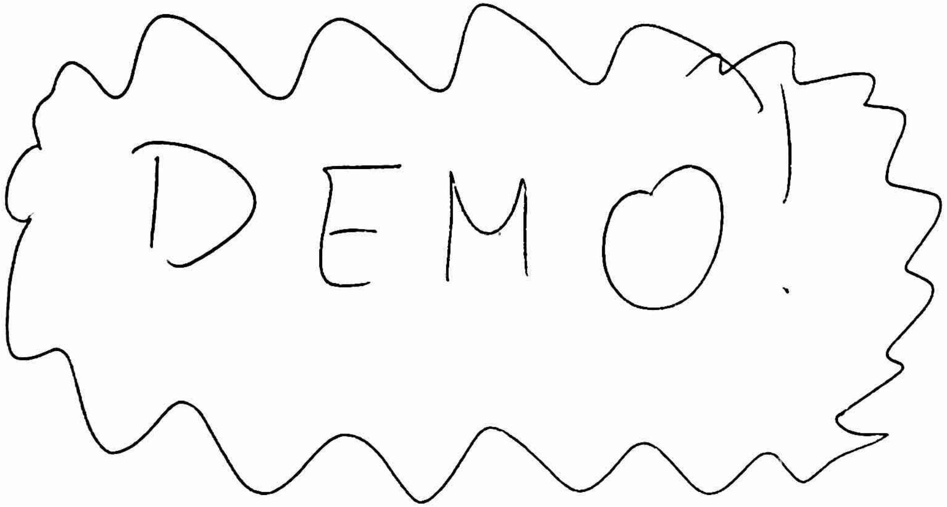
WHY?

→ LEAK TRIGGERED FROM THE REMOTE IS DANGEROUS

DUMB USE CASE - MINERVA - LIB

- SYSCALL FUZZING USING RANDOM VALUES





DUMB FUZZER IS DUMB

RUMP FUZZ - FILESYSTEMS

APPROACH: MOUNT FS → DO SOME OPERATIONS → UNMOUNT

TESTED EXT2, FFS AND FOUND DOZEN OF CRASHES

DEMO

RUMPFUZZ - NETWORK

① APPROACH #1 → INJECT PACKETS USING RAW SOCKETS

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 : ≈10K/s USING PERSISTENT AFL MODE

PROBLEMS: ☹ CHECKSUMS, STATEFUL PROTOS, MBUFS, NOT STABLE...

BUGS FOUND...

ZERØ لا شيء Ø

ничего

NADA

UMGANGSSPRACHLICH

RIEN NIC

何もない

...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

BLUETOOTH

... MORE

- OSS-FUZZ INTEGRATION
- IMPROVE COVERAGE
- OTHER OSes? LibOS?

WE NEED YOU!

THANKS:

POOKA - ANTTI KANTEE

MICHAŁ DARDAS & LOGICALTRUST

#NETBSD-QA @ FREENODE

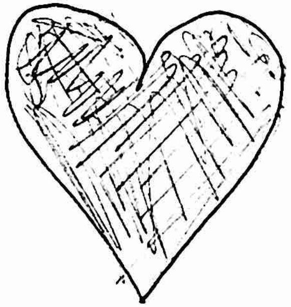
ETERNAL

RYOSHU - KAMIL RYTAROWSKI

MRG

THE NETBSD DEVELOPERS

DRAGONFLY TEAM



DISCUSSION

~~Q&A~~

FELL FREE TO CONTACT ME

SHM@NetBSD.org

M.KOCIELSKI@LOGICALTRUST.NET

#netbsd-qa @ FREENODE

shm @ FREENODE