The Container Security in Healthcare Data Exchange System

Bachelor's degree graduation project

Chih-Hsuan Yang

National Sun Yat-sen University
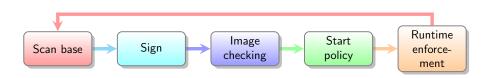Advisor: Chun-I Fan

August 13, 2021

Outline

1 Last week

2 This week

Flow chart

Plans in this week

- Use the BPF feature and fuzzing technique to collect the "normal" system calls in healthcare data exchange system.
- Keep survey those papers.

Last week

- (e)BPF is a dynamic tracing technique.
- The bpf() system call first appeared in Linux 3.18.
- The kernel provide a JIT that can execute out Byte Code probe into the kernel dynamically.

cannot attach kprobe, probe entry may not exist


```
→  foo cat ./clone.py && sudo ./clone.py

    File: ./clone.py

 1   #!/usr/bin/env python3
 2   from bcc import BPF
 3
 4   # bpf program in restricted C language.
 5   prog = """
 6   int hello_world(void *ctx) {
 7       bpf_trace_printk("Hello, World!\\n");
 8       return 0;
 9   }
10   """
11
12   b = BPF(text=prog)
13
14   # attaching hello_world function to sys_clone system call.
15   b.attach_kprobe(event="sys_clone", fn_name="hello_world")
16
17   # reading from /sys/kernel/debug/tracing/trace_pipe
18   b.trace_print(fmt="Program:{0} Message:{5}")
19
```

```
→  foo cat /boot/config-$(uname -r) | grep "CONFIG_.*BPF" | sed '/#/d' | grep .
CONFIG_CGROUP_BPF=y
CONFIG_BPF=y
CONFIG_BPF_LSM=y
CONFIG_BPF_SYSCALL=y
CONFIG_ARCH_WANT_DEFAULT_BPF_JIT=y
CONFIG_BPF_JIT_DEFAULT_ON=y
CONFIG_IPV6_SEG6_BPF=y
CONFIG_NETFILTER_XT_MATCH_BPF=m
CONFIG_NET_CLS_BPF=m
CONFIG_NET_ACT_BPF=m
CONFIG_BPF_JIT=y
CONFIG_BPF_STREAM_PARSER=y
CONFIG_LWTUNNEL_BPF=y
CONFIG_HAVE_EBPF_JIT=y
CONFIG_BPF_EVENTS=y
CONFIG_TEST_BPF=m
→  foo cat /boot/config-$(uname -r) | grep "CONFIG_IKHEADERS"
# CONFIG_IKHEADERS is not set
→  foo
```

```
cannot attach kprobe, probe entry may not exist
Traceback (most recent call last):
  File "/media/d/foo/./clone.py", line 15, in <module>
    b.attach_kprobe(event="sys_clone", fn_name="hello_world")
  File "/usr/lib/python3/dist-packages/bcc/__init__.py", line 683, in attac
h_kprobe
    raise Exception("Failed to attach BPF program %s to kprobe %s" %
Exception: Failed to attach BPF program b'hello_world' to kprobe b'sys_clon
e'
```

Recompile the kernel


```
→  foo cat /boot/config-$(uname -r) | grep -f bpf.conf; uname -a
CONFIG_BPF=y
CONFIG_HAVE_EBPF_JIT=y
CONFIG_BPF_SYSCALL=y
CONFIG_BPF_JIT=y
CONFIG_IKHEADERS=y
CONFIG_NET_CLS_BPF=m
CONFIG_NET_ACT_BPF=m
CONFIG_BPF_EVENTS=y
Linux scc-home 5.13.7 #3 SMP Tue Aug 3 23:13:49 CST 2021 x86_64 GNU/Linux
→  foo
```

But it still not work, which has same error as previous.

Another front-end wrapper bpftrace

```
→  foo sudo bpftrace --version
bpftrace v0.13.0-63-g341b
free(): double free detected in tcache 2
[1]    157002 abort      sudo bpftrace --version
→  foo
```

```
[ 78%] Built target watchpoint
[ 99%] Built target man_man
[100%] Built target adoc_man
[100%] Built target man
Install the project...
-- Install configuration: "Release"
-- Up-to-date: /usr/local/bin/bpftrace
-- Up-to-date: /usr/local/share/bpftrace/tools/bashreadline.bt
→  build git:(master) /usr/local/bin/bpftrace --version
bpftrace v0.13.0-63-g341b
free(): double free detected in tcache 2
[1]    162171 abort      /usr/local/bin/bpftrace --version
→  build git:(master)
```

bpftrace using docker


```
Step 11/11 : ENTRYPOINT ["/bin/sh", "/build.sh"]
 ---> Using cache
 ---> 9fd441beb718
Successfully built 9fd441beb718
Successfully tagged bpftrace-builder-alpine:latest
/media/d/foo/bpftrace
CMake Warning at CMakeLists.txt:46 (message):
  static libc is known to cause problems, consider STATIC_LIBC=OFF.  Procee
d
  at your own risk


-- Please install the libbfd development package (missing: LIBBFD_LIBRARIES
 LIBBFD_INCLUDE_DIRS)
-- Please install the libopcodes development package (missing: LIBOPCODES_L
IBRARIES LIBOPCODES_INCLUDE_DIRS)
-- Found LLVM 9.0.0: /usr/lib/llvm9/lib/cmake/llvm
-- Disabled codegen test for LLVM != 12
CMake Error at /usr/share/cmake/Modules/FindPackageHandleStandardArgs.cmake
:137 (message):
  Could NOT find GTest (missing: GTEST_LIBRARY GTEST_MAIN_LIBRARY)
Call Stack (most recent call first):
  /usr/share/cmake/Modules/FindPackageHandleStandardArgs.cmake:378 (_FPHSA_
FAILURE_MESSAGE)
  /usr/share/cmake/Modules/FindGTest.cmake:197 (FIND_PACKAGE_HANDLE_STANDAR
D_ARGS)
  tests/CMakeLists.txt:107 (find_package)


-- Configuring incomplete, errors occurred!
See also "/media/d/foo/bpftrace/build-release/CMakeFiles/CMakeOutput.log".
See also "/media/d/foo/bpftrace/build-release/CMakeFiles/CMakeError.log".
→ bpftrace git:(master)
□ 0  ↑ 22h 55m      1 zsh
```

https://hackmd.io/@25077667/Byvwszd1K#bpftrace-using-docker

The official document says

- `./build-docker-image.sh` - builds just the `bpftrace-builder` Docker image
- `./build-debug.sh` - builds bpftrace with debugging information (requires `./build-docker-image.sh` to have already been run)
- `./build-release.sh` - builds bpftrace in a release configuration (requires `./build-docker-image.sh` to have already been run)

`./build.sh` is equivalent to `./build-docker-image.sh && ./build-release.sh`

Debends on kernel version and distro.

林易緯
之前在嘗試該範例時也有遇到問題，我記得有與 syscall 在某個版本的重命名有關，我當時是更換成 trace __x64_sys_clone

可以透過 cat /proc/kallsyms | grep sys_clone 看看可以追蹤的 kernel symbol

讚 · 回覆 · 分享 · 1天

楊志璿
林易緯 thanks, i will try it in a few minutes.
讚 · 回覆 · 分享 · 1天

楊志璿
林易緯 你是對的，謝謝
讚 · 回覆 · 分享 · 1天

Jim Huang 管理員
請改進你的「漢語」表達，例如「已時間成本考量」這陳述到底表達什麼？你也該說清楚，自己用什麼 Linux distribution、如何重現問題 (你可利用虛擬機器)，再來。這個討論區有 4500+ 人，你若能夠先在本文 (即上方的提問) 清楚陳述，會有更多高手願意查看 HackMD 筆記內容，從而給你更多指引，這也才有討論的效益。

讚 · 回覆 · 分享 · 1天

楊志璿
Jim Huang 時間成本考量：希望在兩天內解決問題
Distro. : Debian 11
讚 · 回覆 · 分享 · 1天

Jim Huang 管理員
為何不書寫清楚呢？文字導向的訊息也不該用圖片表示，對資訊檢索無異，更對視覺障礙的朋友不友善
讚 · 回覆 · 分享 · 1天

楊志璿
Jim Huang Got it, I will make it better! Thanks.
讚 · 回覆 · 分享 · 1天

Many debugs...

- The kernel what I compiled is 5.13.7.
- Hey, there are no 'linux-headers-$(uname -a)' in debian sid!
- Okay, I can compile the header my my self.
- Hey, the bcc and bpftrace are failed, they cannot get those entry on 5.13.7.
- Okay, I go to fix the bcc and bpftrace source code, and it works on host OS.
- Hey, It does not work in container, failed to compile BPF module. (Next page)
- Okay, I change the front end of eBPF to tracee, which is another open source wrapper.
- It also works on host OS, but failed to load libbpf in container. (Next page)

```
→ foo sudo docker run --rm -v $(pwd)/data:/app/data bcc_try
/virtual/main.c:29:1: warning: declaration of 'struct tracepoint__raw_syscalls__sys_exit' will not be visible outside of this function [-Wvisibility]
TRACEPOINT_PROBE(raw_syscalls, sys_exit) {
^
/virtual/include/bcc/helpers.h:1263:46: note: expanded from macro 'TRACEPOINT_PROBE'
int tracepoint__##category##_##event(struct tracepoint__##category##_##event *args)
                                            ^
<scratch space>:153:1: note: expanded from here
tracepoint__raw_syscalls__sys_exit
^
/virtual/main.c:50:19: error: incomplete definition of type 'struct tracepoint__raw_syscalls__sys_exit'
    u32 key = args->id;
              ~~~~^
/virtual/main.c:29:1: note: forward declaration of 'struct tracepoint__raw_syscalls__sys_exit'
TRACEPOINT_PROBE(raw_syscalls, sys_exit) {
^
/virtual/include/bcc/helpers.h:1263:46: note: expanded from macro 'TRACEPOINT_PROBE'
int tracepoint__##category##_##event(struct tracepoint__##category##_##event *args)
                                            ^
<scratch space>:153:1: note: expanded from here
tracepoint__raw_syscalls__sys_exit
^
1 warning and 1 error generated.
Traceback (most recent call last):
  File "./syscount.py", line 165, in <module>
    bpf = BPF(text=text)
  File "/usr/lib/python2.7/dist-packages/bcc/__init__.py", line 452, in __init__
    raise Exception("Failed to compile BPF module %s" % (src_file or "<text>"))
Exception: Failed to compile BPF module <text>
  foo
```

```
→ dist sudo docker run --rm -v $(pwd)/data:/app/data
root@838d1a85ff3b:/# app
app
root@838d1a85ff3b:/# app/tracee-ebpf
libbpf: failed to open system Kconfig
libbpf: failed to load object 'embedded-core'
2021/08/05 17:46:45 error creating Tracee: failed to l
root@838d1a85ff3b:/#
```

There also have some distro. dependency issue

- Alpine
- Debian stretch, buster, bulleyes
- Ubuntu Bionic, Focal Fossa
- Linux kernel version, 4.18.0, 5.2.0. . .

This week

Can work on "Simple" test case

```python
#!/usr/bin/python3

print("Hello world!")
```

src/hello.py

We didn't catch the 'write' system call, that is if there is a process called 'write'.

It's invalid operation. Even though it is a common system call.

Move the ebpf bin to the FHIR Env.


```
→  ~ docker exec -it 02 bash
bash-4.4$ cat /etc/os-release
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
ID="rhel"
ID_LIKE="fedora"
VERSION_ID="8.4"
PLATFORM_ID="platform:el8"
PRETTY_NAME="Red Hat Enterprise Linux 8.4 (Ootpa)"
ANSI_COLOR="0;31"
CPE_NAME="cpe:/o:redhat:enterprise_linux:8.4:GA"
HOME_URL="https://www.redhat.com/"
DOCUMENTATION_URL="https://access.redhat.com/documentation/red_hat_enterprise_linux/8/"
BUG_REPORT_URL="https://bugzilla.redhat.com/"

REDHAT_BUGZILLA_PRODUCT="Red Hat Enterprise Linux 8"
REDHAT_BUGZILLA_PRODUCT_VERSION=8.4
REDHAT_SUPPORT_PRODUCT="Red Hat Enterprise Linux"
REDHAT_SUPPORT_PRODUCT_VERSION="8.4"
bash-4.4$
```

```
→  ~ docker run -d ibmcom/ibm-fhir-server:latest
Unable to find image 'ibmcom/ibm-fhir-server:latest' locally
latest: Pulling from ibmcom/ibm-fhir-server
5f6bf015319e: Pull complete
45cc8b7f2b43: Pull complete
87212cfd39ea: Pull complete
b89ea354ae59: Extracting  143.7MB/203MB
5627e846e80f: Download complete
e2bef77118c7: Download complete
d3cbf41efb4e: Download complete
4a939b72e1c6: Download complete
4feff1abc28e: Download complete
9ff4465d271b: Download complete
5e41012b4001: Download complete
410af8b678f6: Download complete
2f26dc40d01f: Download complete
1415c9c2e161: Download complete
94d978ce0b1f: Download complete
e374de62001e: Download complete
1fabae8675b6: Download complete
7b088cbebf16: Download complete
4167c1ebbd85: Download complete
```

```
→  ~ python
Python 3.9.6 (default, Jun 30 2021, 10:22:16)
[GCC 11.1.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> (2/3)**19
0.000451092989732578
>>>
```

```
→  FHIR git:(trace) ✗ docker run --rm -it fhir-trace bash
bootstrap.sh - [INFO]: 2021-08-13_01:59:08 - Current directory: /opt/ibm-fhir-server
bootstrap.sh - [INFO]: 2021-08-13_01:59:08 - Skipping Derby database bootstrapping
[root@36e1f03c66b9 defaultServer]# ldd /tracee/tracee-ebpf
        linux-vdso.so.1 (0x00007fff97b22000)
        libelf.so.1 => /lib64/libelf.so.1 (0x00007fcc4b696000)
        libz.so.1 => /lib64/libz.so.1 (0x00007fcc4b47f000)
        libc.musl-x86_64.so.1 => not found
        libc.so.6 => /lib64/libc.so.6 (0x00007fcc4b0ba000)
        /lib/ld-musl-x86_64.so.1 => /lib64/ld-linux-x86-64.so.2 (0x00007fcc4b8af000)
[root@36e1f03c66b9 defaultServer]# /app/trace_run.sh
-rwxr-xr-x 1 root root 15M Aug  3 21:05 /tracee/tracee-ebpf
Error loading shared library libelf.so.1: No such file or directory (needed by /tracee/tracee-e
bpf)
Error loading shared library libz.so.1: No such file or directory (needed by /tracee/tracee-ebp
f)
Error relocating /tracee/tracee-ebpf: elf_getdata: symbol not found
Error relocating /tracee/tracee-ebpf: gzopen: symbol not found
Error relocating /tracee/tracee-ebpf: elf_end: symbol not found
Error relocating /tracee/tracee-ebpf: gelf_getehdr: symbol not found
Error relocating /tracee/tracee-ebpf: elf_memory: symbol not found
Error relocating /tracee/tracee-ebpf: elf_getshdrstrndx: symbol not found
Error relocating /tracee/tracee-ebpf: gelf_getsym: symbol not found
Error relocating /tracee/tracee-ebpf: elf_rawdata: symbol not found
Error relocating /tracee/tracee-ebpf: elf_nextscn: symbol not found
Error relocating /tracee/tracee-ebpf: gzclose: symbol not found
Error relocating /tracee/tracee-ebpf: elf_ndxscn: symbol not found
Error relocating /tracee/tracee-ebpf: elf_version: symbol not found
Error relocating /tracee/tracee-ebpf: gelf_getshdr: symbol not found
Error relocating /tracee/tracee-ebpf: elf_errmsg: symbol not found
Error relocating /tracee/tracee-ebpf: elf_getscn: symbol not found
Error relocating /tracee/tracee-ebpf: gelf_getrel: symbol not found
Error relocating /tracee/tracee-ebpf: gzgets: symbol not found
Error relocating /tracee/tracee-ebpf: elf_begin: symbol not found
Error relocating /tracee/tracee-ebpf: gelf_getclass: symbol not found
Error relocating /tracee/tracee-ebpf: elf_strptr: symbol not found
```

Lisense issue? self-build!

Well. . .

3 problems to be solve

1. Kernel version
2. Dynamic linking issue: musl, libelf
3. Has it enough time to fuzz?