

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 6, 2021

Outline

1 Plans

2 (e)BPF

Flow chart



Plans

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.

I did my best.
But it still have some problems.
Do you want to listen it?

(e)BPF

- (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\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 attach_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_clone'
```

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)
```

bpfftrace using docker

```

Step 11/11 : ENTRYPOINT ["/bin/sh", "/build.sh"]
--> Using cache
--> 9fd441beb718
Successfully built 9fd441beb718
Successfully tagged bpfftrace-builder-alpine:latest
/media/d/foo/bpfftrace
CMake Warning at CMakeLists.txt:46 (message):
  static libc is known to cause problems, consider STATIC_LIBC=OFF. Proceed
  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/bpfftrace/build-release/CMakeFiles/CMakeOutput.log".
See also "/media/d/foo/bpfftrace/build-release/CMakeFiles/CMakeError.log".
-> bpfftrace git:(master)
0 22h 55m 1 zsh

```

<https://hackmd.io/@25077667/Byvwszd1K#bpfftrace-using-docker>

The official document says

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

```
bpfftrace git:(master) sudo ./build-debug.sh
CMake Warning at CMakeLists.txt:46 (message):
  static libc is known to cause problems, consider STATIC_LIBC=OFF.
  d
  at your own risk

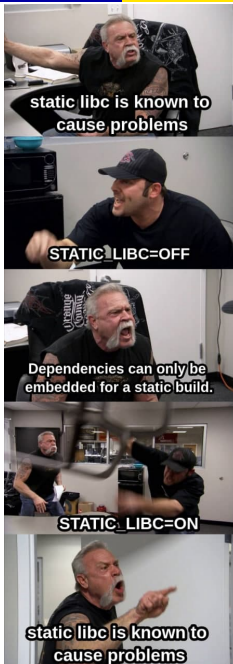
-- Please install the libbpf development package (missing: LIBBPF_LIBRARY
LIBBPF_INCLUDE_DIRS)
-- Please install the libopcodes development package (missing: LIBOPCODES
LIBRARIES LIBOPCODES_INCLUDE_DIRS)
-- Found LLVM 9.0.0: /usr/lib/llvm9/lib/cmake/llvm
-- Disabled codegen test for LLVM != 12
CMake Error at /usr/share/cmake/Modules/FindPackageHandleStandardArg
: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 (
FAILURE_MESSAGE)
  /usr/share/cmake/Modules/FindGTest.cmake:197 (FIND_PACKAGE_HANDLE
D_ARGS)
  tests/CMakeLists.txt:107 (find_package)

-- Configuring incomplete, errors occurred!
See also "/media/d/foo/bpfftrace/build-debug/CMakeFiles/CMakeOutput.l
See also "/media/d/foo/bpfftrace/build-debug/CMakeFiles/CMakeError.lo
bpfftrace git:(master)
```

```
bpfftrace git:(master) x ./b
CMake Error at CMakeLists.txt:
Dependencies can only be emb

Enable STATIC_LINKING=ON to

-- Configuring incomplete, err
See also "/tmp/bpfftrace/build-
See also "/tmp/bpfftrace/build-
bpfftrace git:(master) x
```



Depends 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



2



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 bpfttrace are failed, they cannot get those entry on 5.13.7.
- Okay, I go to fix the bcc and bpfttrace 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

```

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000

36°C | 06:01 | 05 Aug | scc scc-home

```

+ 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, bullseyes
- Ubuntu Bionic, Focal Fossa
- Linux kernel version, 4.18.0, 5.2.0...

```

327
328  #if LINUX_VERSION_CODE < KERNEL_VERSION(4, 18, 0)
version.h /usr/include/linux - 宣告 (1)
1  #define LINUX_VERSION_CODE 330286
2  #define KERNEL_VERSION(a,b,c) (((a) << 16) + ((b) << 8) + ((c) > 255 ? 255 : (c)))
3
34  # DOCKER_BUILDER_KERN_SRC_MNT is the kernel headers directory to mount into the docker builder container. DOCKER_BUILDER_KERN_SRC sh
35  DOCKER_BUILDER_KERN_SRC_MNT ?= $(dir $(DOCKER_BUILDER_KERN_SRC))
36  LINUX_VERSION_CODE := $(shell uname -r | gawk '{split($0,a,"."); split(a[3], b, "-"); print lshift(a[1], 16) + lshift(a[2],8) + b[1]
37

```