Step Up Your Game with strace

PA Hackers

Nov 20, 2019

Mike Salvatore

ESM Tech Lead/Security Engineer

CANONICAL ubuntu

Who Am I?

Mike Salvatore

- Education
  - B.S. Electrical Engineering, Rutgers University
  - M.S. Cybersecurity, Johns Hopkins University
- Current employment
  - Ubuntu Security Team at Canonical
- Contact
  - mike.salvatore@canoncal.com
  - msalvatore on the freenode IRC network
  - @L0n3_W0lf on the PA Hackers Slack

Join us!

Engage with PA Hackers on Slack.

https://join.slack.com/t/pahackers/shared_invite/enQtNDYwOTk5NTc2OTc4LTg1ZmU2ZGMyNDAwMGMyZjkwMDVhNjU2ODI1MDYzODgzMmQxM2M3Y2Q4MzkxNjAxZjIwYTA3OGExZDAxZmFmYWY

Contents

Strap in!

We’re going **deep** down the rabbit hole.

Meet Colonel Kernel

What is the kernel?

“The kernel is a computer program that is the core of a computer's operating system, with complete control over everything in the system.” [1]

What stops application from taking over?

The kernel does many things.

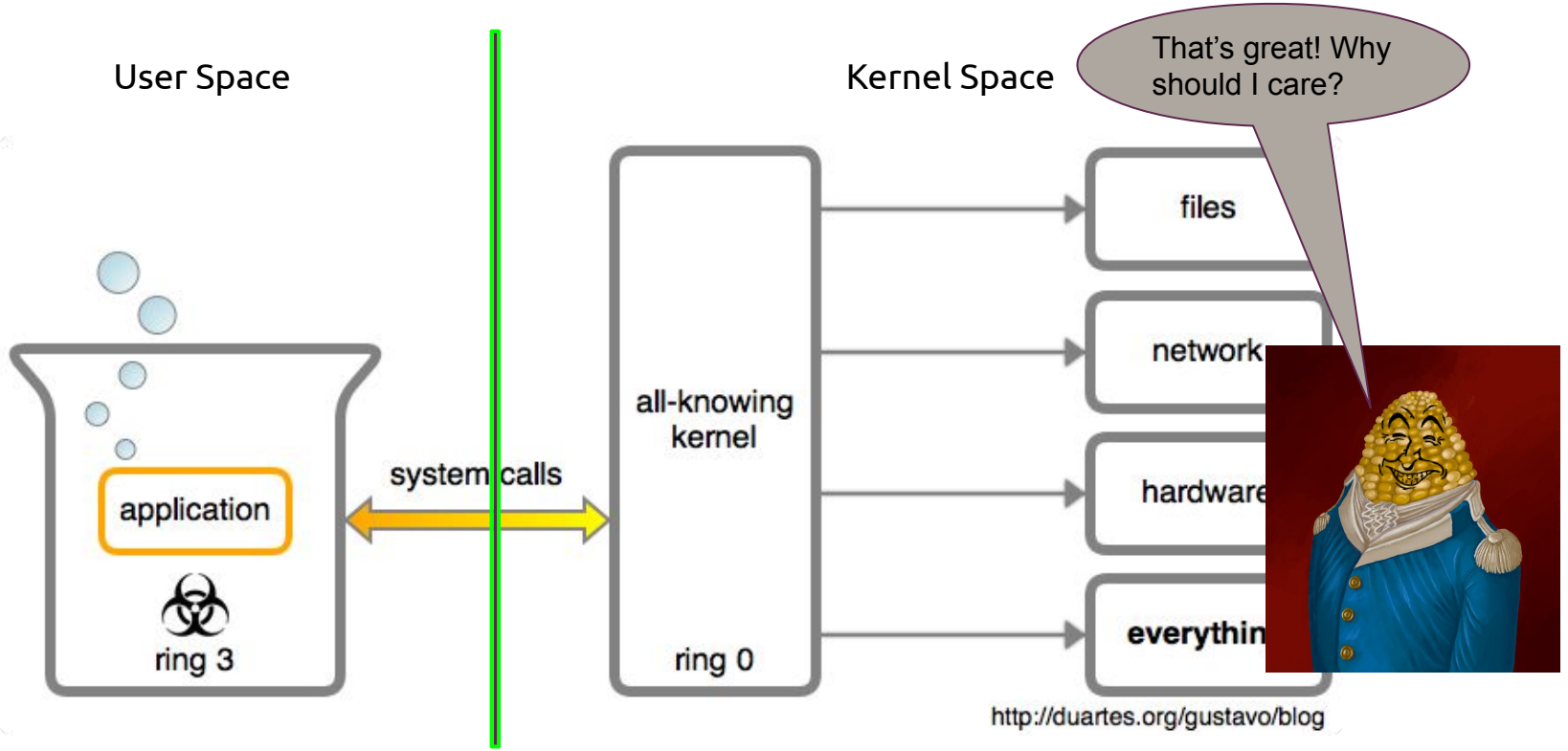
For this talk:

The kernel enforces security boundaries and serves as an intermediary between applications and hardware.

System Calls

“System calls are the fundamental interface between an application and the Linux kernel.” [2]

System Calls



If I could observe system calls...

- I could:
  - Find out what resources a program is accessing.
  - Determine what a program is **actually** doing.
  - Debug issues in record time.
  - Convince my colleagues that I'm a wizard.

strace

Strace is a tool available on Linux that records and displays all of the system calls that a process makes.

Some strace Use Cases

- Help! My application is frozen.
- I got a cryptic error about some kind of failure.
  - It says to check the log for more info. Where is the log?
  - I don’t know where this thing loads its config from.
- Why is my application so slow?
- My application invokes another application incorrectly, resulting in an error.
  - How is the 2nd application being invoked?
- I want to create an application that does something similar to but slightly different from an existing application.
  - How does the existing application do it?
- My application sends some data over the network.
  - What is it actually trying to send?
  - Is the data being sent at all?

$> strace cat /tmp/hello.txt

Live demo!

Useful Arguments (see `man strace`)

-f -- Trace child processes as they are created by currently traced processes

-o FILENAME -- Write the trace output to the file filename rather than to stderr

-e trace=SET -- Trace only the specified set of system calls.

-e trace=%file -- Trace all system calls which take a file name as a argument.

Note: There are many other prebuilt filters. See `man strace`.

-t, -tt -- Prefix each line of the trace with the wall clock time with increasing precision.

-T -- Show the time spent in system calls (useful for profiling an application)

-c -- Count time, calls, and errors for each system call and report a summary on program exit, suppressing the regular output.

Good commands to trace

ls

ln

pwd

nc

nmap

echo

cat

man

free

top

curl

mkdir

rm

lsof

modprobe

insmod

rmmod

ps

dd

uptime

uname

df

du

chmod/chown

mv

touch

Key Takeaways

- System calls are the fundamental interface between an application and the Linux kernel.
- *Most* of the interesting things an application does utilize the system call interface.
- strace shows you all of the system calls an application makes
  - This tells you *what* the application is doing, but it may still be unclear *why* it's doing certain things.
- When interpreting the output of strace, `man 2 [SYSCALL]` will tell you what a system call does and how it is invoked.
- Using strace can teach you important things about how your operating system works.
  - I recommend you use strace to observe 1 command per day for 30 days. This will teach you more than any college class or certification.

How I Use strace at work

Using Strace in a Security Context

Security Vulnerability Emails

- As a member of the Ubuntu Security Team, one of my responsibilities is to respond to emails regarding vulnerabilities in Ubuntu or Ubuntu's packages.
- As a result, I get emails from strangers that look like this:

Subject: Vulnerability in Blah-Blah

From: randomstranger@randomdomain.com

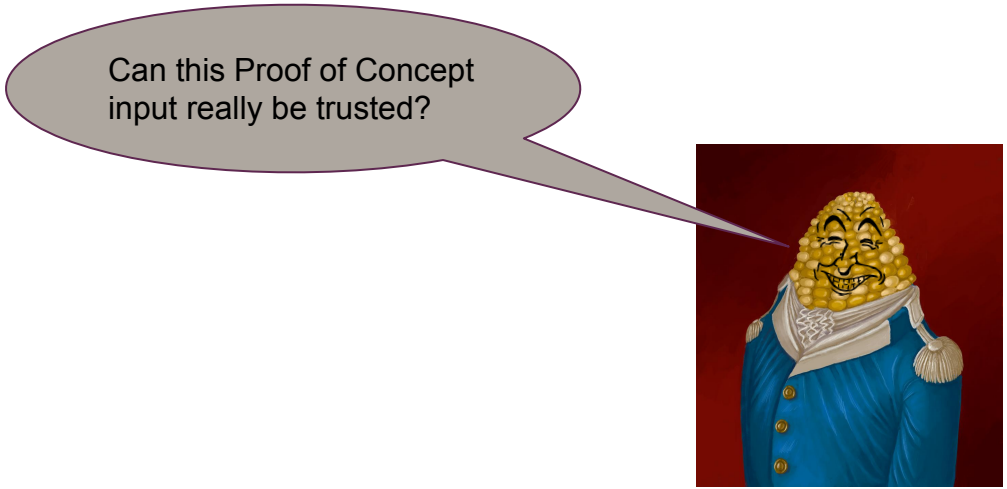
Hi Mike,

I found a potential security vulnerability in package *blah-blah*. If you use *blah-blah* to process the attached proof of concept input, you'll see that it will cause *blah-blah* to (freeze|crash|segfault|transport you to another dimension).

Thanks,
A Concerned User/Researcher

Safely Processing This PoC

- Scan with malware scanner
- Run in VM on dedicated hardware
- Firewall between test machine and other systems
- Reformat drive after verification of vulnerability
- Some secret tricks



You guessed it: strace to the rescue!

Live Demo!

Relevant strace Results

```
213 openat(AT_FDCWD, "my_ebook.epub", O_RDONLY) = 3
214 read(3, "PK\3\4\24\0\0\0\10\0\354hgOH\7\36'Q\2\0\0\345\2\0\0009\0\34\0.."..., 8191) = 1192
215 stat("/tmp/6f72/../../../../../../../../home/goodguy/.ssh", {st_mode=S_IFDIR|0700, st_size=4096, ...}) = 0
216 stat("/tmp/6f72/../../../../../../../../home/goodguy/.ssh/authorized_keys", {st_mode=S_IFREG|0600, st_size=741, ...})      = 0
217 openat(AT_FDCWD, "/tmp/6f72/../../../../../../../../home/goodguy/.ssh/authorized_keys", O_WRONLY|O_CREAT|O_TRUNC, 0666) = 4
218 write(4, "ssh-rsa AAAAB3NzaC1yc2EAAAADAQAB"..., 741) = 741
…
282 openat(AT_FDCWD, "/tmp/6f72-048b-d694-ec75-f793-bc52-8970-251b/EPUB/package.opf", O_RDONLY) = 3
283 read(3, "<?xml version=\"1.0\" encoding=\"UT"..., 49152) = 880
284 read(3, "", 45056)                       = 0
285 read(3, "", 49152)                       = 0
286 --- SIGSEGV {si_signo=SIGSEGV, si_code=SEGV_MAPERR, si_addr=NULL} ---
287 +++ killed by SIGSEGV (core dumped) +++
```

2 Hit Super Combo!

- To gain remote access on the victim, the attacker combines two vulnerabilities
  - CVE-2019-13032 - Null Pointer Dereference
  - CVE-2019-13241 - Zip Slip
- The first vulnerability tricks the victim into thinking they understand the effect of the malformed epub, while the second vulnerability delivers the knockout blow.
- By using strace, we can understand what the exploit *actually* does, not what we're told it does.

Some strace Use Cases

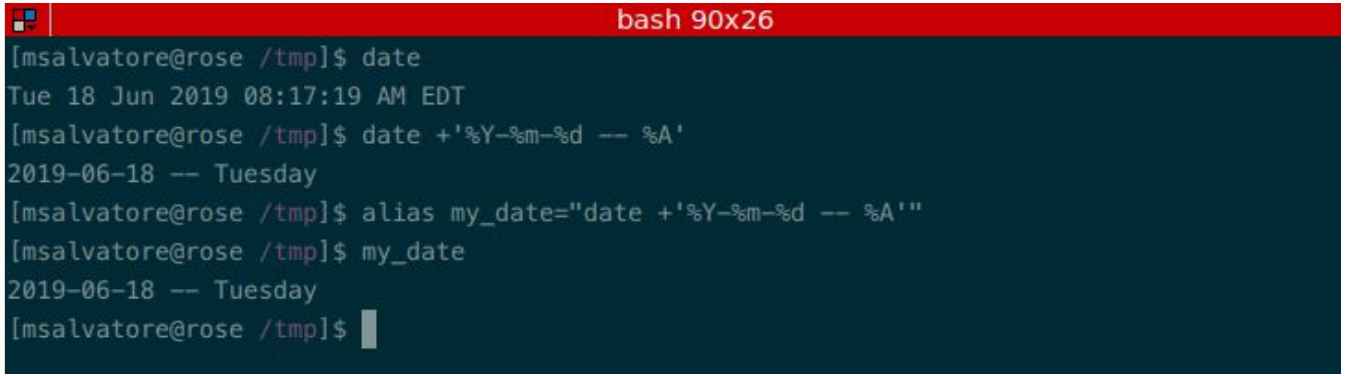
- Help! My application is frozen.
- I got a cryptic error about some kind of failure.
  - I don't know where this thing loads its config from.
  - It says to check the log for more info. Where is the log?
- Why is my application so slow?
- My application invokes another application incorrectly, resulting in an error.
  - How is the 2nd application being invoked?
- I want to create an application that does something similar to but slightly different from an existing application.
  - How does the existing application do it?
- My application sends some data over the network.
  - What is it actually trying to send?
  - Is the data being sent at all?
- Reverse Engineering/Malware Analysis

Using strace for Mischief

The Dark Side of the Force

Aliases

Put simply, a bash alias is an abbreviation or nickname for another command. You define aliases using the “alias” builtin.



Favorite Alias

I have a lot of aliases.

By far, this one is my favorite:

$> alias emacs=vim

Storing Aliases for Later Use

The ~/.bashrc file gets sourced every time you start bash. Adding aliases to this file will make them available to you in every new bash instance.

The PATH environment variable

The PATH environment variable contains a list of directories that contain executables. When you invoke any executable on the command line, bash searches the directories listed in your PATH to find the executable.

An improperly configured PATH (or one modified by an attacker) can trick you into executing malicious code.

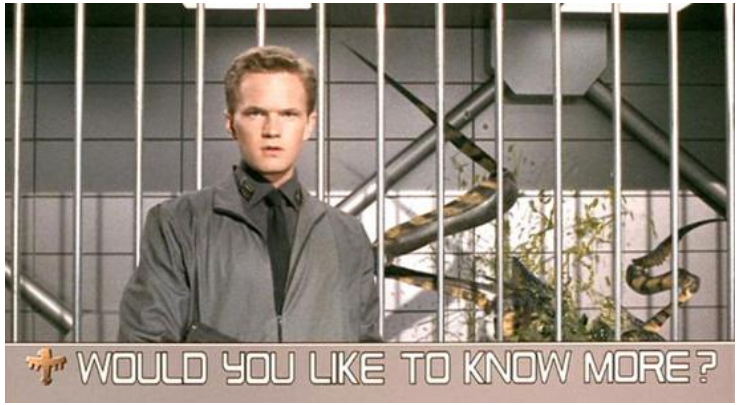
Live Demo

But how does strace work?

You can always use strace to trace strace!

Further Reading

- http://www.brendangregg.com/blog/2014-05-11/strace-wow-much-syscall.html
- http://www.brendangregg.com/blog/2015-07-08/choosing-a-linux-tracer.html
- https://jvns.ca/blog/2015/04/14/strace-zine/
- https://dev.to/captainsafia/say-this-five-times-fast-strace-ptrace-dtrace-dtruss-3e1b
- https://salvatoresecurity.com/fun-with-fuzzers-or-how-i-discovered-three-vulnerabilities-part-1-of-3/
- https://github.com/PAHackers/Presentations/tree/master/How%20to%20type%20less%20with%20bash




GO FORTH
AND STRACE
imgflip.com

Thank you. Questions?