Google

Verified Boot with BPF

Neill Kapron <nkapron@google.com>

May 2024

Background

Goal: Modern BPF in Android

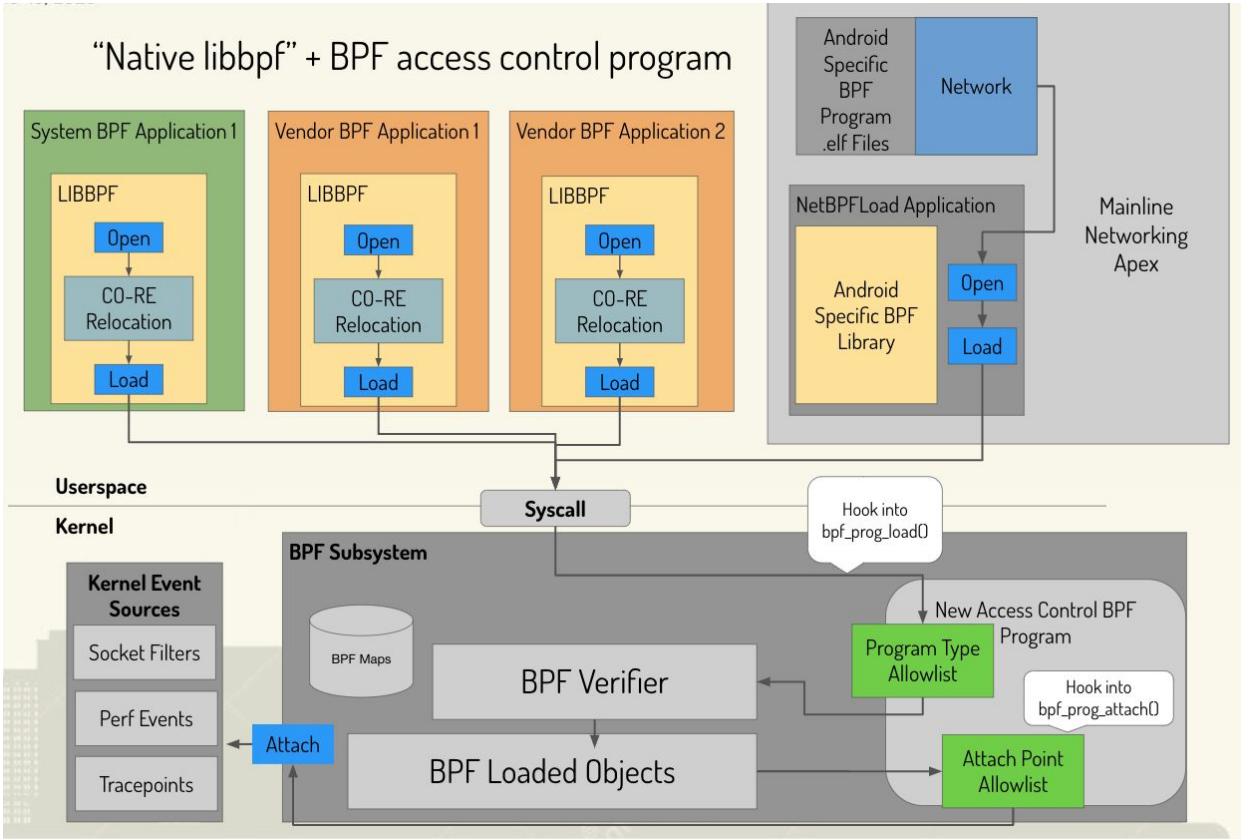
Three BPF user stories: Networking, System, Vendor

Separate update/release timelines for each user story

Long term compatibility

New Android versions must run on previous Android kernels

LSM Proposal from LPC23

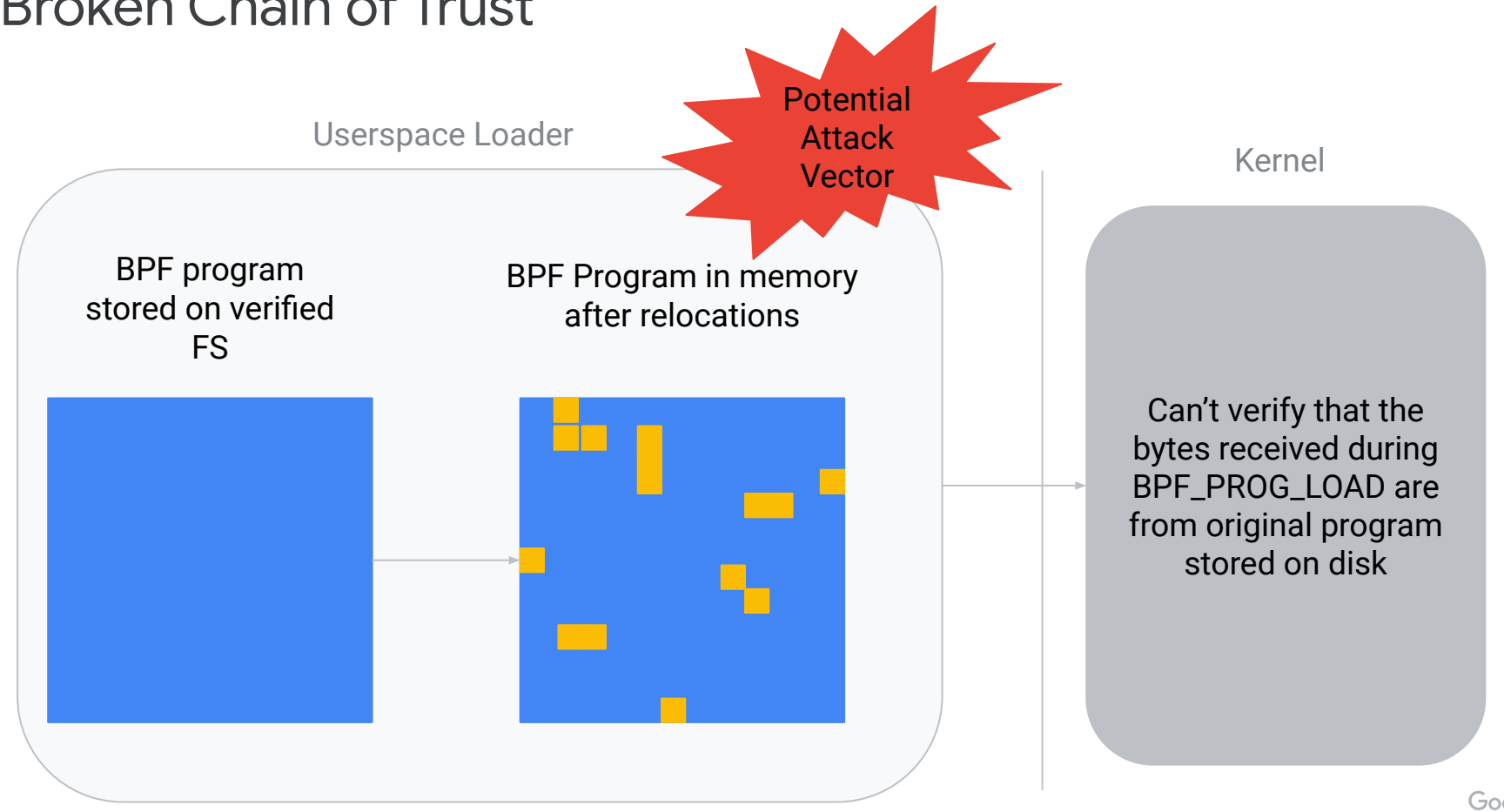


For more information, see the LPC23 presentation: https://lpc.events/event/17/contributions/1599

Security Review:

“That sounds great, but it must maintain verified boot.”

Broken Chain of Trust



Approaches considered

Single trusted loader (Android) (1)

Signed shared library objects

Relocation playbook

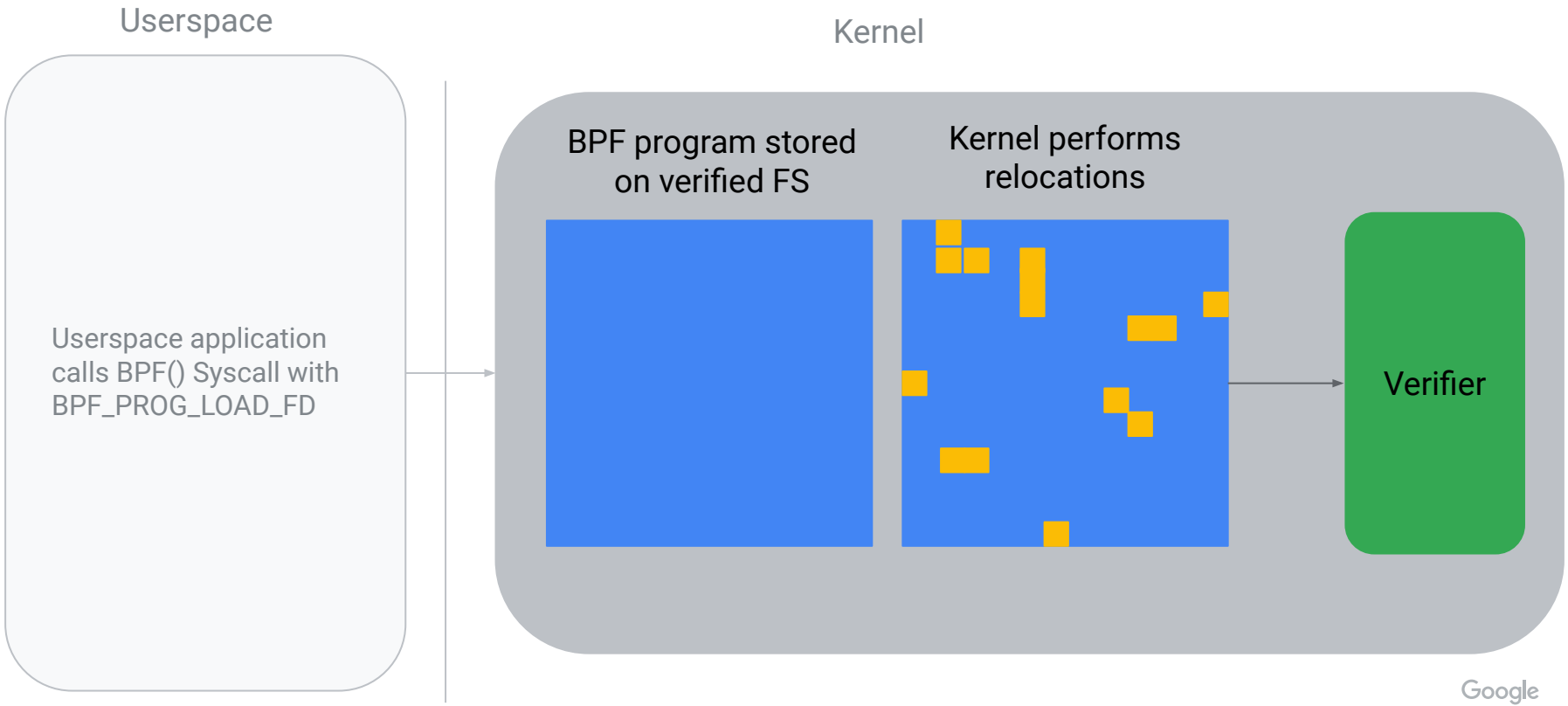
Light skeleton

BPF Signing using fsverity (Lorenz Bauer) (2)

1. https://cs.android.com/android/platform/superproject/+/master:system/bpf/bpfloader/BpfLoader.cpp
2. http://vger.kernel.org/bpfconf2023_material/Lorenz_Bauer_-_BPF_signing_using_fsverity_and_LSM_gatekeeper.pdf

BPF_PROG_LOAD_FD

Established Chain of Trust



Moving loader functionality to the kernel

Extend the BPF syscall with BPF_PROG_LOAD_FD

Userspace passes a file descriptor to the kernel

Kernel opens the ELF file

Parse ELF

Create Maps

Pass programs to verifier

Reality of moving loader functionality to the kernel

Extend the BPF syscall with BPF_PROG_LOAD_FD

Userspace passes a file descriptor to the kernel

Kernel opens the ELF file

Validates ELF format

Parse ELF

Create Maps

Perform Map relocations

BTF

CO-RE

Pass bytecode to verifier

...

Dependency Resolution

Kernel provides zlib: include/linux/zlib.h

Limited ELF handling found in:

- fs/binfmt_elf.c
- kernel/kexec_elf.c
- kernel/module/main.c
- others…

Benefits

Enables the verified boot path

Signature verification could be implemented for use on non-signed filesystems

Focused loader development (currently each library must provide their own)

Resolves potential library incompatibility stories

Eases the BPF preload story

Questions

How does this manage BPF object lifecycle?

What is the syscall return value?

BPF ELF format specification

Compatibility story (How does this translate to other BPF runtimes?)

BPF ELF format

BPF ELF format

Documentation/bpf/btf.rst - Defines .BTF, .BTF.ext sections
Libbpf: Documentation/bpf/libbpf/program_types.rst

eBPF ELF Profile Specification, v0.1 (Dave Thaler):
ietf.org/archive/id/draft-thaler-bpf-elf-00.html

Questions/Comments?