K-Miner: Uncovering Memory Corruption in Linux

David Gens, Simon Schmitt, Lucas Dava, Ahmad-Reza Sadeghi

Motivation

- static analysis faces severe scalability challenges
- All analysis frameworks for kernel code are limited to intra-procedural analysis
- Linux comprises over 24 million lines of code

Contributions

- Enable global static analysis for kernel code
  - K-Miner(inter-procedural static analysis)
- prototype framework implementation
  - on top of LLVM
- extensive evaluation
  - apply it to all system calls across many different Linux versions

Background

- Data-Flow analysis

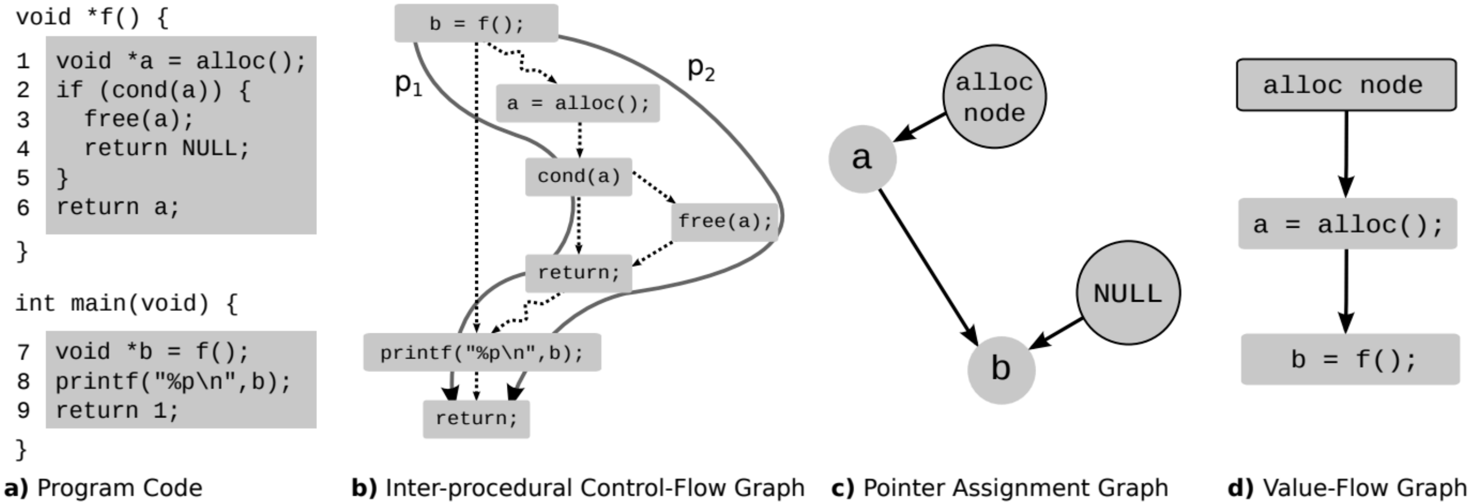

Figure 1: Data-flow analyses utilize graphs to reason about program behavior at compile time.

Background

- Memory-corruption vulnerabilities
  - integer overflows(IO)
  - use-after-free(UAF)
  - dangling pointers(DP)
  - double free(DF)
  - buffer overflow(BO)
  - missing pointer checks(MPC)

K-Miner

- Assumptions
  - attacker has control user-space
  - OS is isolated from user processes
  - Adversary cannot insert malicious code into the kernel
- Goal
  - Systematically scan the system call interface for these vulnerabilities

Overview

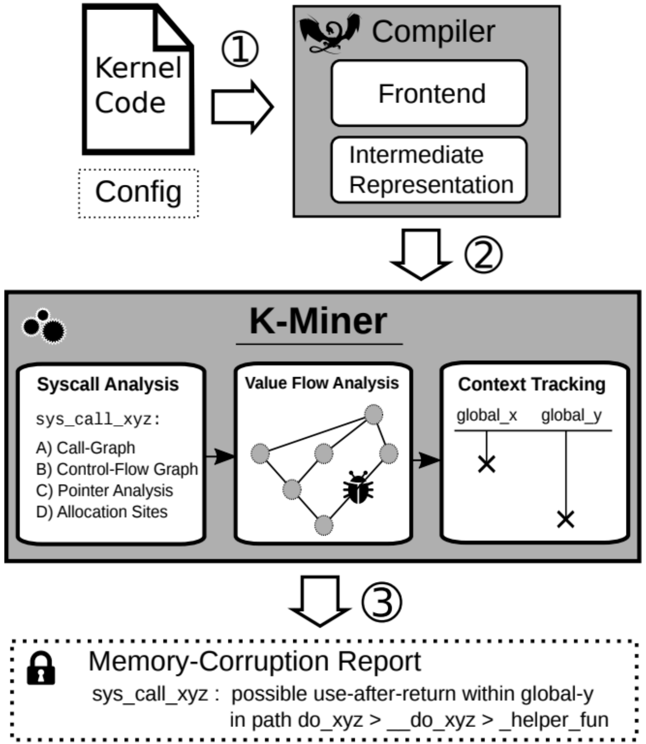

Figure 2: Overview of the different components of K-Miner.

Implementation

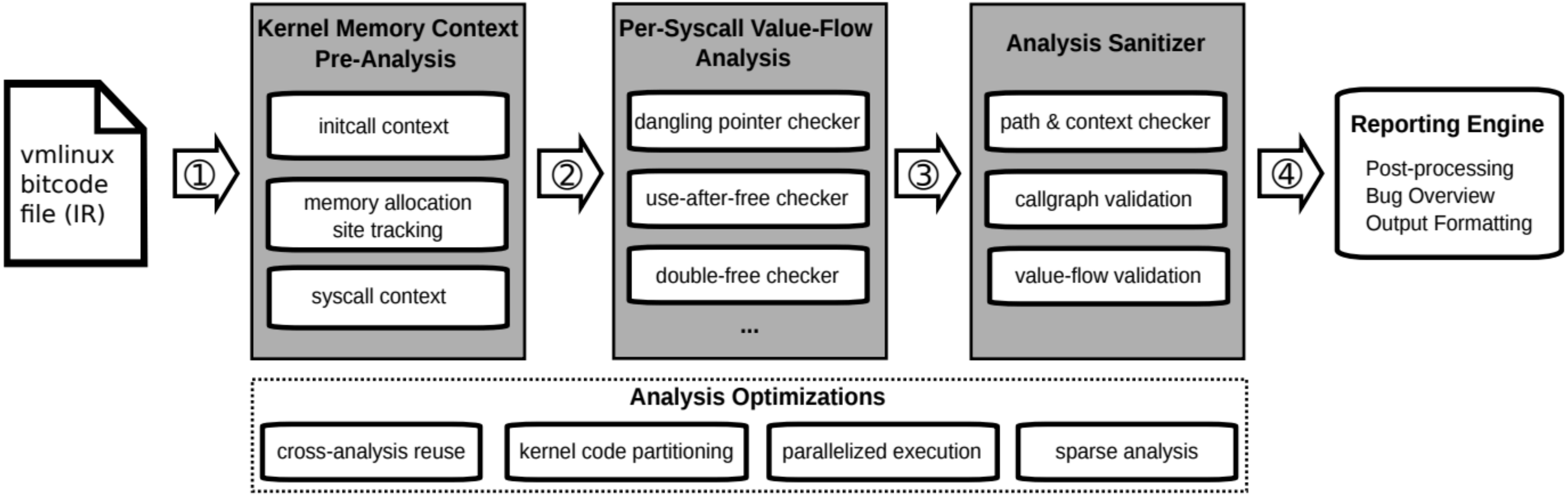

Figure 3: Overview of the K-Miner implementation: we conduct complex data-flow analysis of the Linux kernel in stages, re-using intermediate results.

Evaluation

				Magnitude of Analysis			Report Results		
Version	MLOC	Bitcode	Avg. Run Time	#Functions	#Variables	#Pointers	DP	UAF	DF
3.19	15.5	280M	796.69s	99K	433K	>5M	7 (40)	3 (131)	1 (13)
4.2	16.3	298M	1435.62s	104K	466K	>6M	11 (46)	2 (106)	0 (19)
4.6	17.1	298M	1502.54s	105K	468K	>6M	3 (50)	2 (104)	0 (31)
4.10	22.1	353M	1312.41s	121K	535K	>7M	1 (30)	2 (105)	0 (22)
4.12	24.1	364M	2164.96s	126K	558K	>7.4M	1 (24)	0 (27)	1 (24)

Evaluation

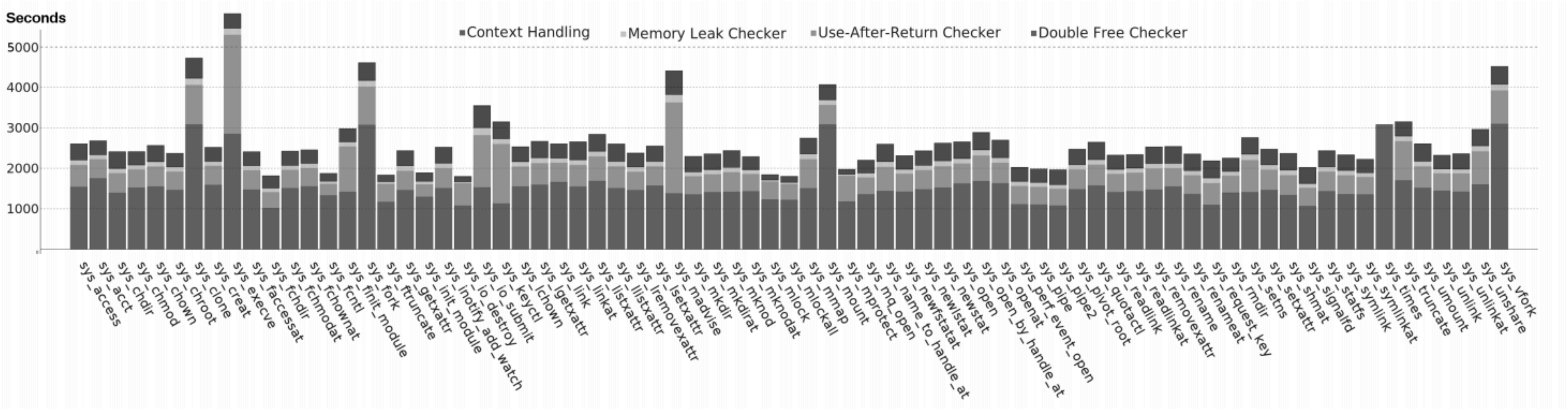

Figure 5: Wall-clock time per analysis phase for system calls requiring more than 30 Minutes within K-Miner.

Evaluation

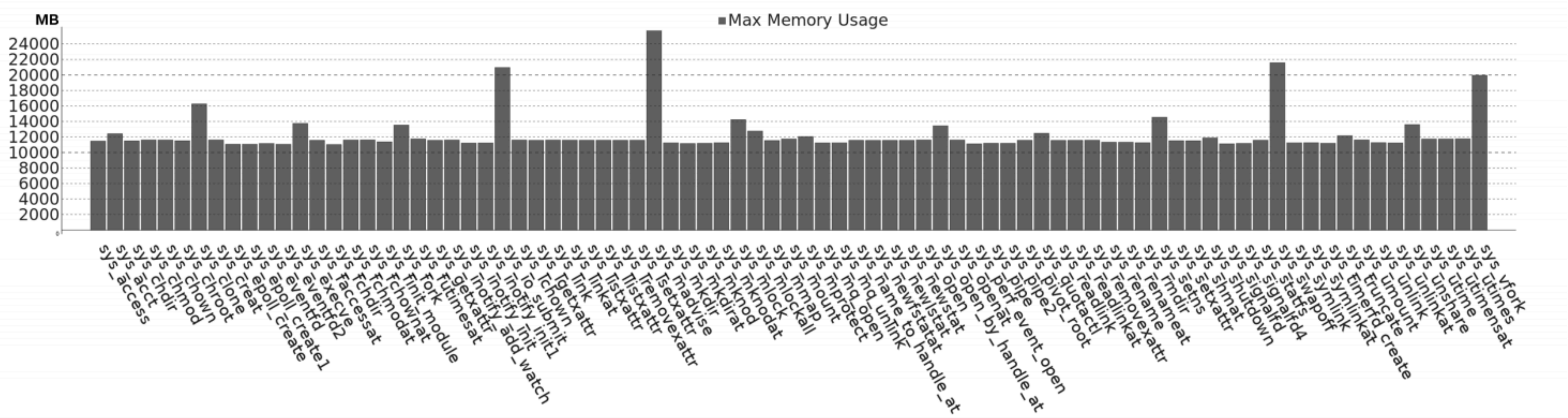

Figure 6: Maximum memory requirements of K-Miner for system calls requiring more than 11G of RAM.