BRIAN JOHANNESMEYER, JAKOB KOSCHEL, KAVEH RAZAVI, HERBERT BOS, & CRISTIANO GIUFFRIDA

KASPER

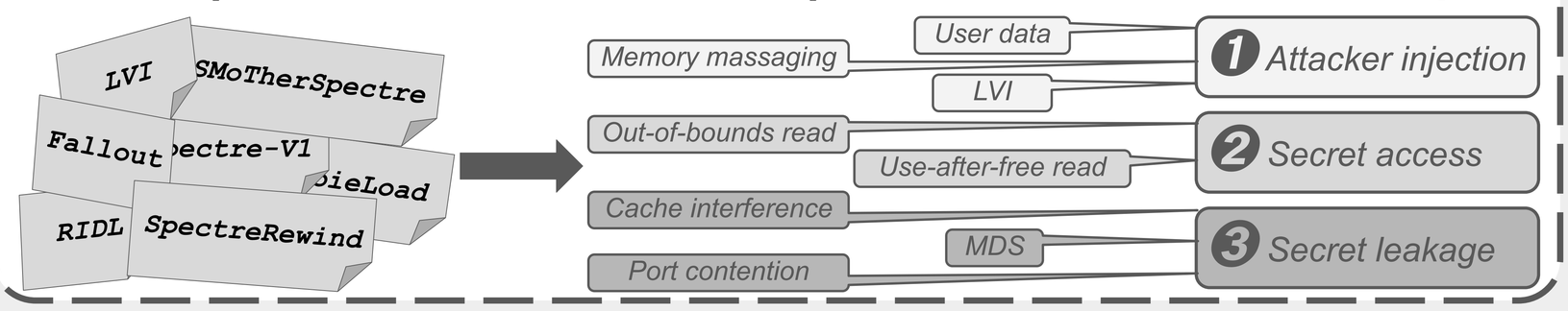
Scanning for Generalized Transient Execution Gadgets in the Linux Kernel

Problem analysis

*Transient execution gadgets are mitigated by **manually** identifying known **gadget patterns**.*

*We can **automatically** identify gadgets by modeling the **generic steps of an attack**.*

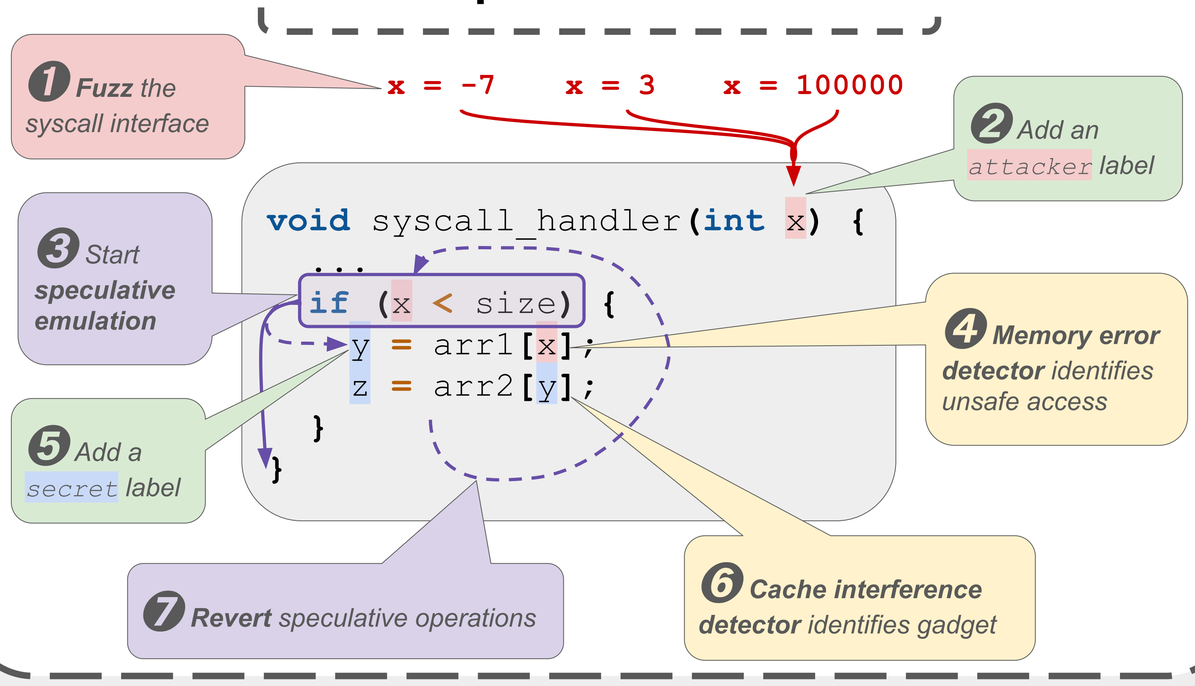
Generalized gadgets



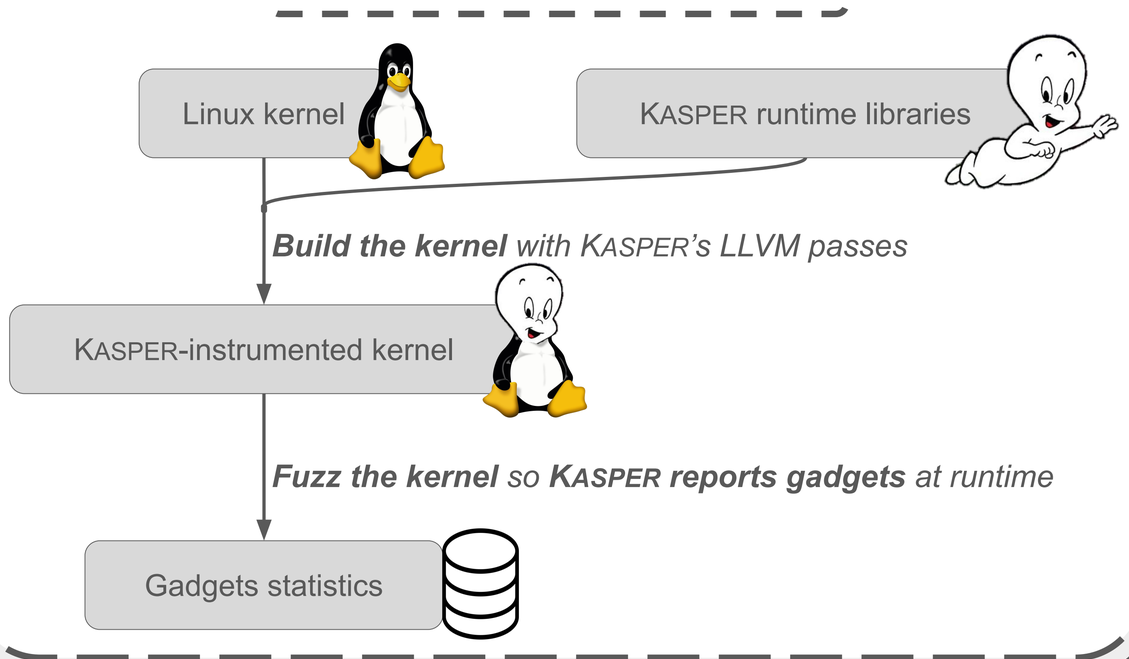
Our solution: KASPER

- ***Model transient execution**: Flip conditional branches at runtime*
- ***Model software/hardware vulnerabilities**: Add runtime checkers*
- ***Model the attack steps**: Use taint policies*
- ***Model an attacker's coverage**: Fuzz the syscall interface*

Example identification



Implementation



Results

Gadgets discovered

Gadget type	Number of reports
USER-CACHE	147
MASSAGE-CACHE	47
LVI-CACHE	12
USER-MDS	600
MASSAGE-MDS	193
USER-PORT	407
MASSAGE-PORT	123
Total	**1379**

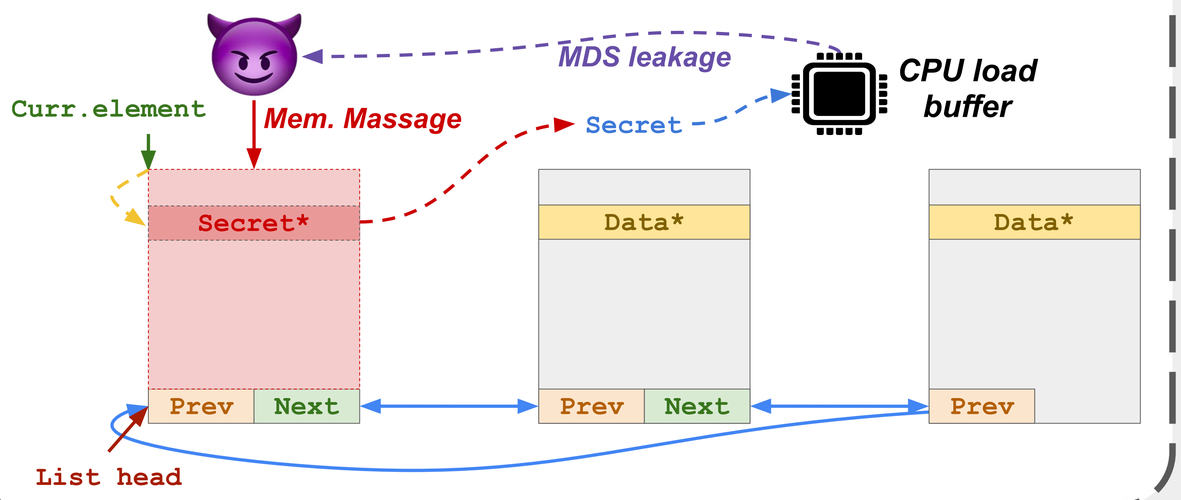
*The original **"Spectre-V1"** remains **largely unmitigated**.*

***LVI is indeed an issue** from a conditional branch misprediction.*

*Transient **memory massaging** is a **legitimate attack vector**.*

*There are a ton of gadgets! But are any of them **actually exploitable**…*

Case Study: Linux's list iterator



*To mitigate the gadgets found, **~90 patches have been accepted** so far.*

*To mitigate the **list iterator** gadget, Linus Torvalds proposed **upgrading the version of C** used by the kernel.*