EPFL

31st Usenix Security Symposium

Midas: Systematic Kernel TOCTTOU Protection

Atri Bhattacharyya, Uros Tesic, Mathias Payer

hexhive

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

ARTIFACT EVALUATED usenix ASSOCIATION REPRODUCED

Kernel Time-of-Check-to-Time-of-Use (TOCTTOU) Bugs

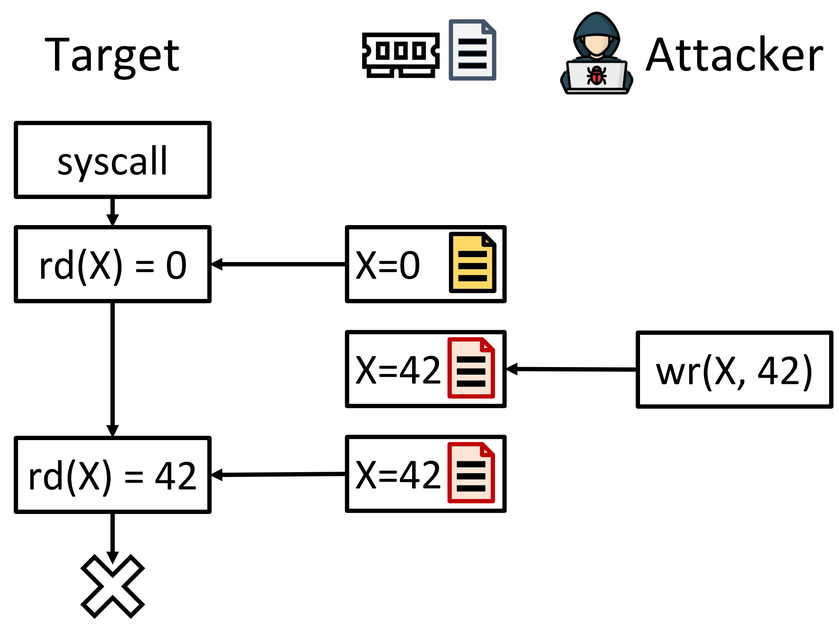
Security critical software has double-fetch bugs
- OS kernels, hypervisors, TEEs

High-impact bugs
- CVE-2016-8438 – "Complete compromise"
- CVE-2020-25212 – "… information disclosure"

Easy to exploit
- Only requires two user threads

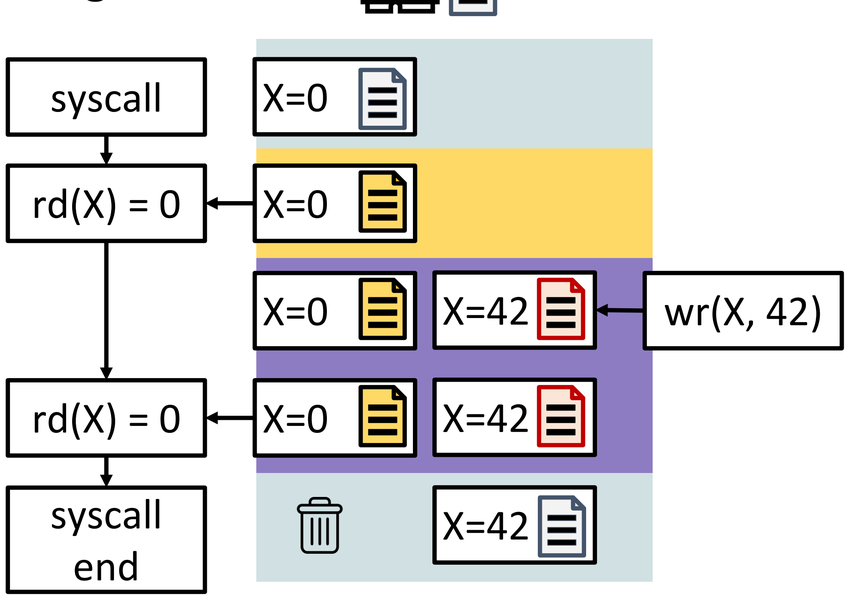
```
sigaction(signum,*act,*oldact)
  if(*(act->X) < len){…}
  …
  access(array[*(act->X)]);
```

Toy TOCTTOU bug



Midas Invariant

"Through a *syscall's lifetime, every read* to a userspace object will return the *same value.*"

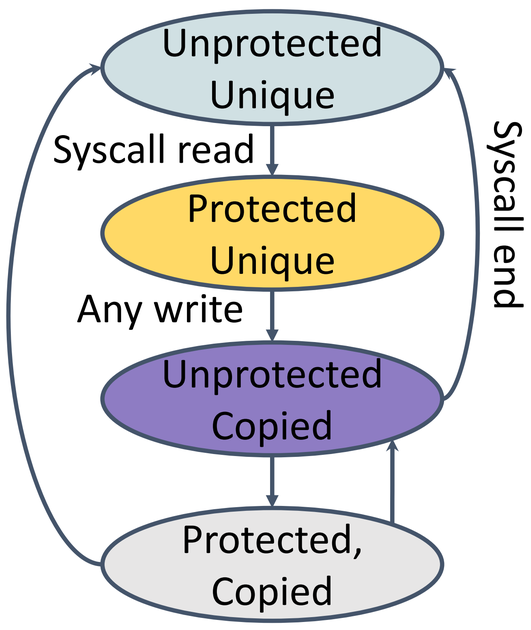


Page State Machine

Transitions:
1. Syscall read → Snapshot
2. Any write → Copy
3. Syscall end → ~~Snapshot~~ ~~Copy~~

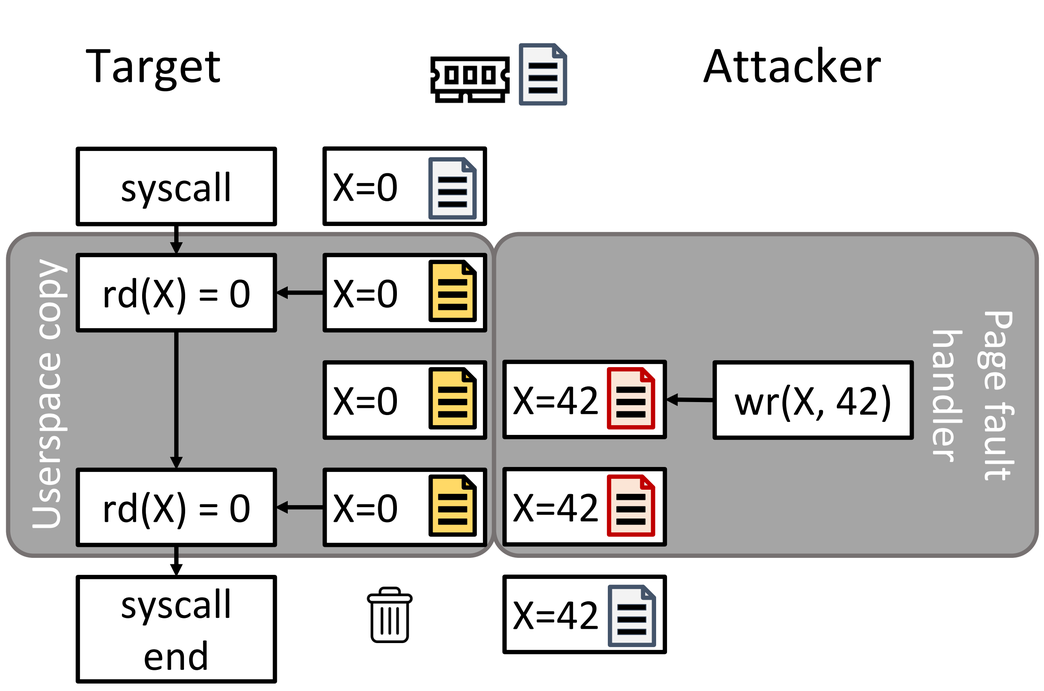
Snapshotting is common (cheap)

(expensive) Copying is rare



Kernel Modifications

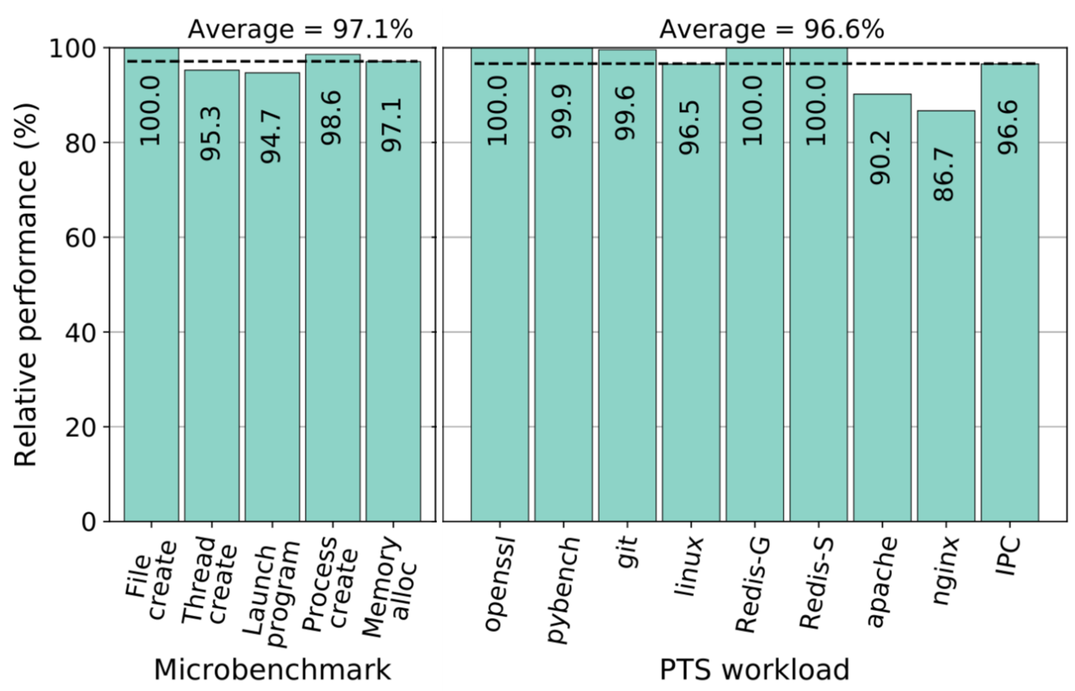
Minimal changes to kernel codebase
- Mostly userspace copy, page fault handler functions
- 17 lines modified, 1100 lines added



Evaluation

Protects against CVE-2016-2516

Low 3.4% average overhead on benchmarks



Partially Sponsored By

Office of Naval Research Science & Technology

European Research Council Established by the European Commission

DARPA