Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

ACSAC, Honolulu, December 11th, 2024

Faking deduplication to prevent timing side-channel attacks on memory deduplication

Jens Lindemann

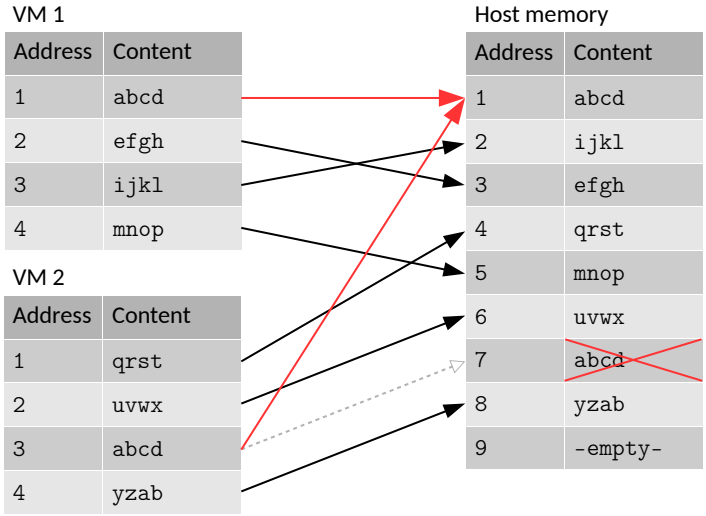
Motivation

- Sharing hardware resources between different services and users more and more popular
- Duplicate memory contents $\rightarrow$ savings potential
- Memory deduplication
  - Removes redundant copies, but
  - opens a side-channel.
- Isolation between control domains (e. g. VMs) broken

Research question

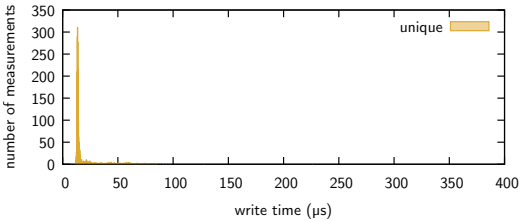
Can we eliminate the side-channel while retaining memory savings?

Memory deduplication

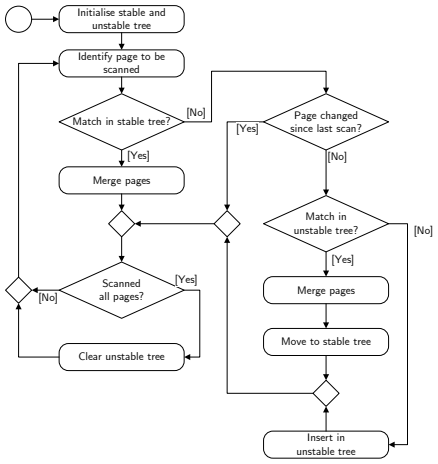


Side-channels based on memory deduplication

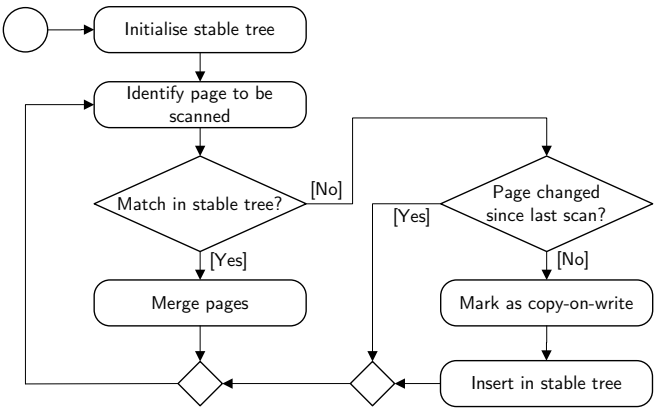
- Deduct whether a page with specific content is present on the system
  - e.g. probe for presence of applications [1]



Linux Kernel Samepage Merging [2]



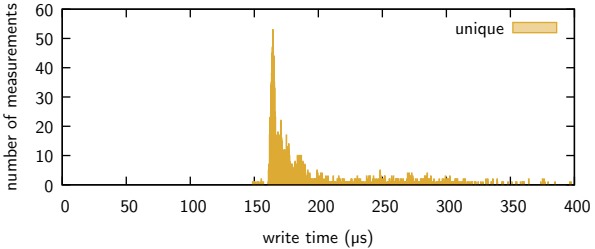
FakeDD – modified KSM implementation

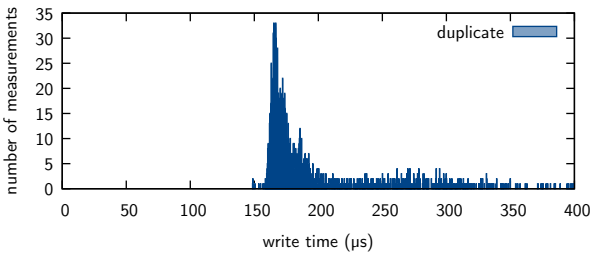


Related work – VUsion [3]

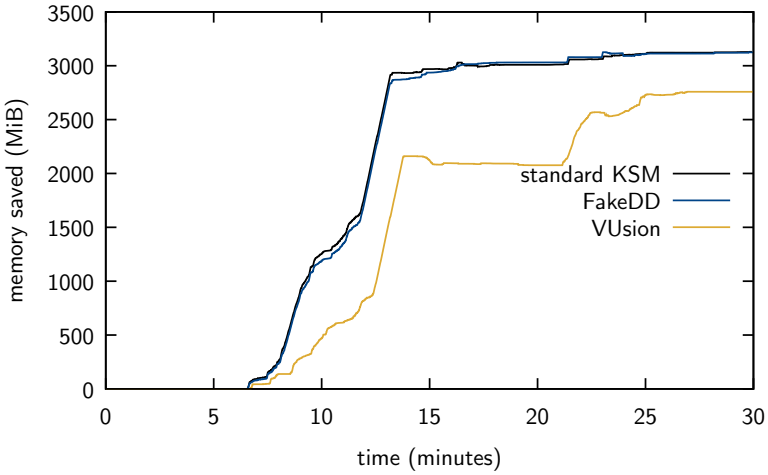
- Also based on Linux KSM
- Implements copy-on-access
  - On pages eligible for deduplication ...
  - ... that it estimates not to be actively used
  - Also affects read operations
- Extended attacker model
  - Attacks relying on read operations, e. g. some Rowhammer-based attacks

Is FakeDD effective in preventing attacks?





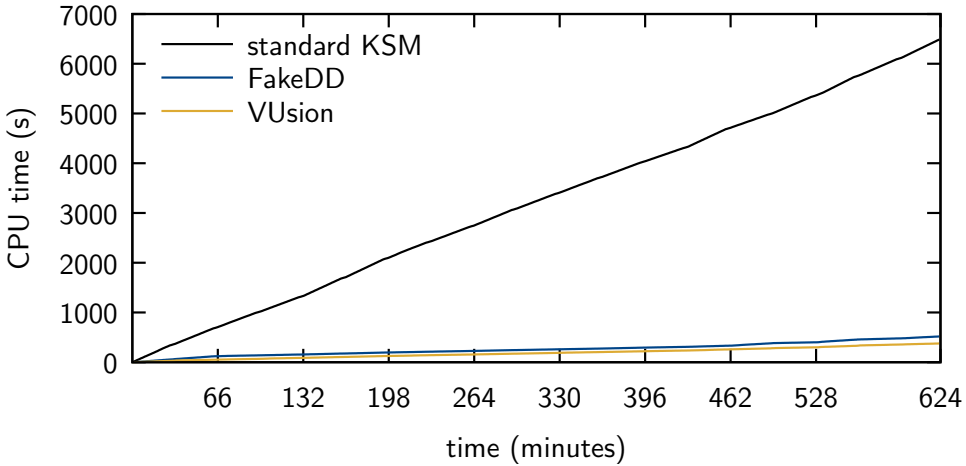
Can FakeDD still save memory?



Application performance

Benchmark	KSM vs. no KSM	FakeDD vs. no KSM	VUsion vs. no KSM
7-Zip compression	-11.81%	-7.39%	-9.65%
memcached	-3.42%	-15.27%	-13.66%
Apache	-14.88%	-11.81%	-12.98%
pmbench (read)	+1.26%	+2.32%	-10.95%
pgbench	-14.54%	-16.69%	-15.76%
x264	-4.96%	-1.62%	-4.07%
Dbench	no statistically significant differences		

CPU consumption of ksmd



Conclusion

- FakeDD can effectively eliminate the side-channel based on write time differences caused by memory deduplication
- Memory savings almost identical to standard KSM
- Acceptable performance overhead
  - Compared to standard KSM: mostly slightly higher or even lower
  - In many scenarios, lower than VUsion (note different attacker model)
- Available as open-source patch for KSM on `https://github.com/jl3/FakeDD`

References

[1] J. Lindemann and M. Fischer, “A memory deduplication side-channel attack to detect applications in co-resident virtual machines,” in *Proceedings of the 33rd Annual ACM Symposium on Applied Computing, SAC 2018*, H. M. Haddad, R. L. Wainwright, and R. Chbeir, Eds. ACM, 2018, pp. 183–192.

[2] A. Arcangeli, I. Eidus, and C. Wright, “Increasing memory density by using KSM,” in *Proceedings of the Linux Symposium*, 2009, pp. 19–28.

[3] M. Oliverio, K. Razavi, H. Bos, and C. Giuffrida, “Secure page fusion with VUsion,” in *Proceedings of the 26th Symposium on Operating Systems Principles*. ACM, 2017, pp. 531–545.