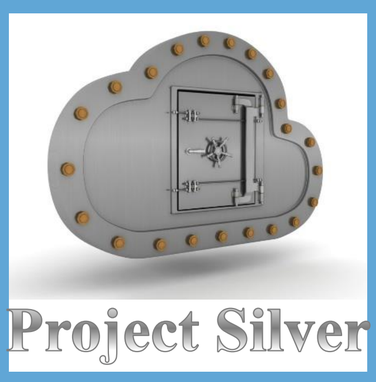


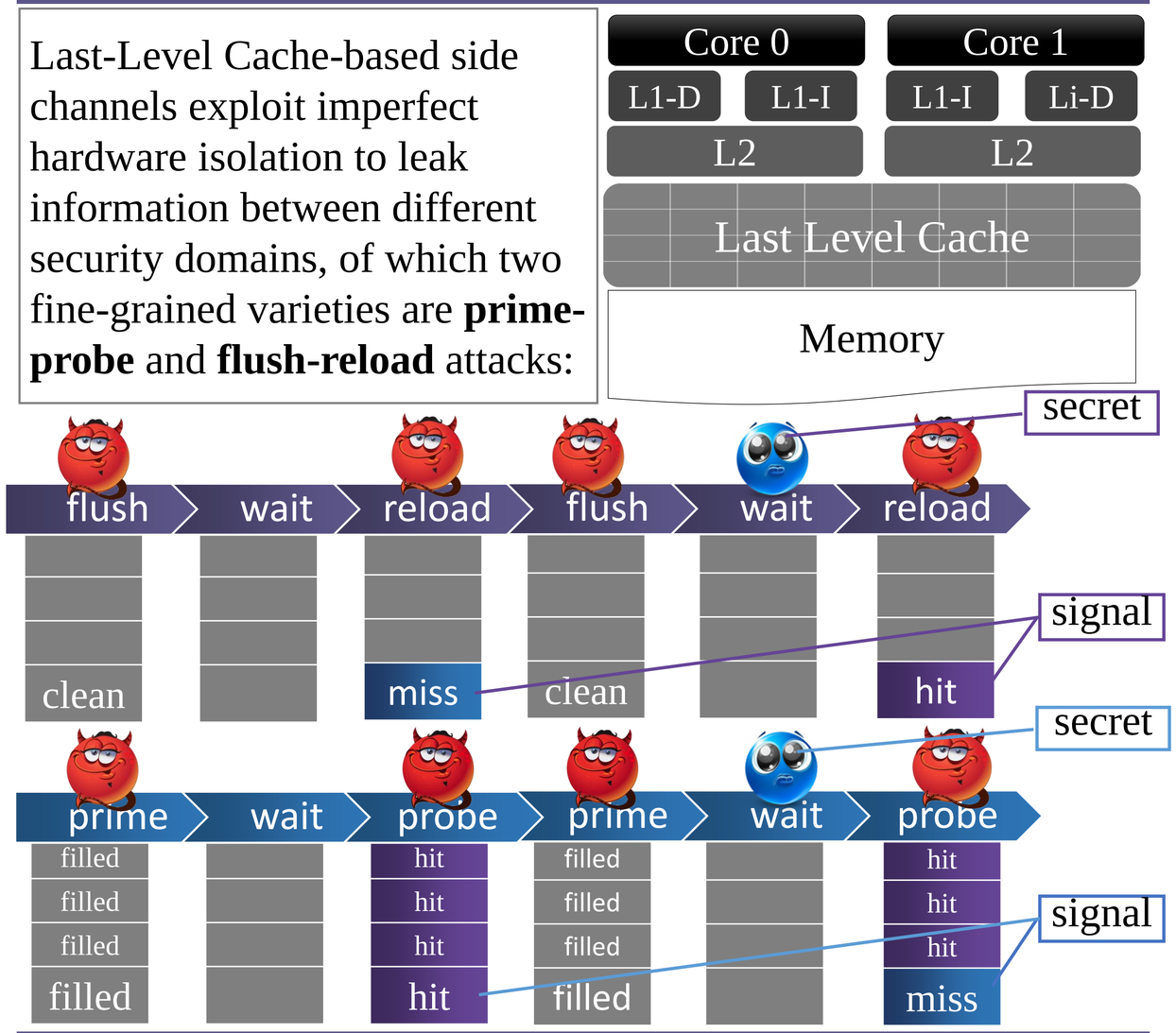
A Software Approach to Defeating Side Channels in Last-Level Caches

Ziqiao Zhou, Michael K. Reiter, Yinqian Zhang

University of North Carolina *ziqiao@cs.unc.edu*

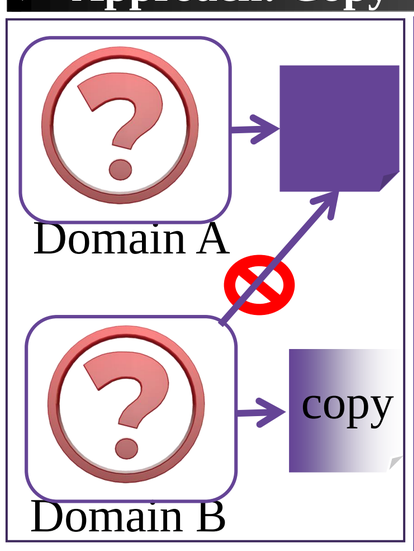
Goals

Last-Level Cache-based side channels exploit imperfect hardware isolation to leak information between different security domains, of which two fine-grained varieties are **prime-probe** and **flush-reload** attacks:

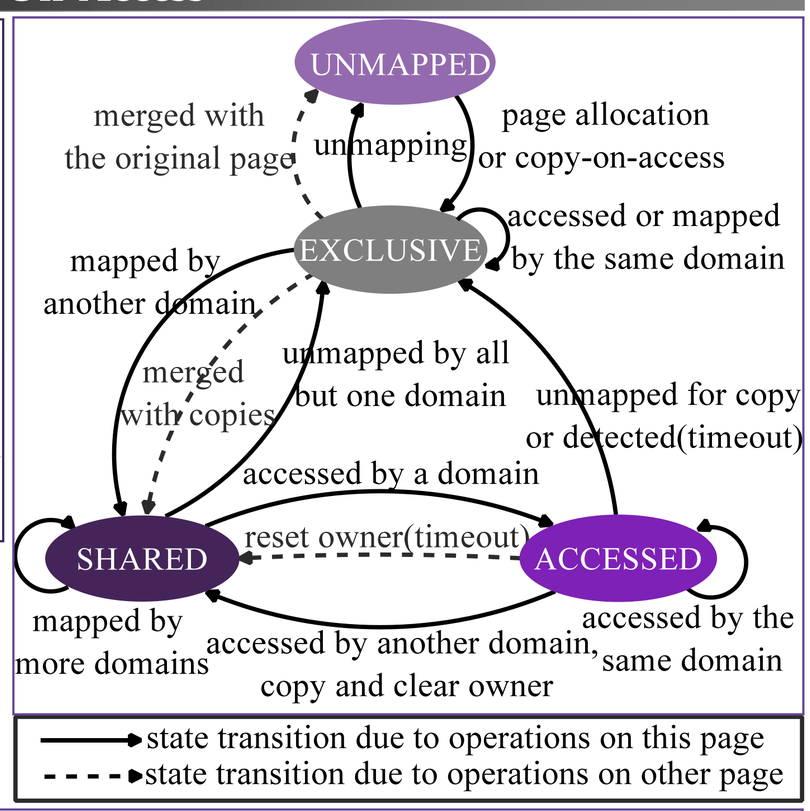


Flush-Reload Defense

➢ Approach: Copy-On-Access



Copy-On-Access uses on-demand copy for other domain's access to disable **active** memory sharing.



To reduce the memory pressure, a daemon will periodically (at a low rate) merge not-recently-used copy, and reset the ownership of page.

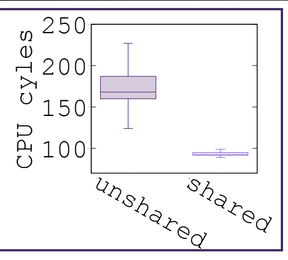
➢ Implementation

Counter		container ID 1	2	3	4	Owner	state
PFN	1	0	0	0	0	NULL	unmapped
	2	2	0	0	0	NULL	exclusive
	3	1	1	1	1	NULL	shared
	4	3	0	1	0	ID 1	accessed

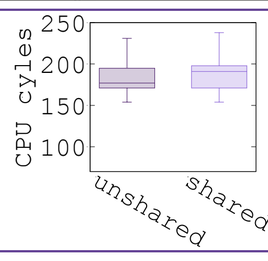
Keep track of page state transition using two data fields: ***counter*** in each ***namespace*** and ***owner*** in each ***page***

➢ Security: reload times, unshared vs. shared memory

Clear signal! CacheBar-disabled



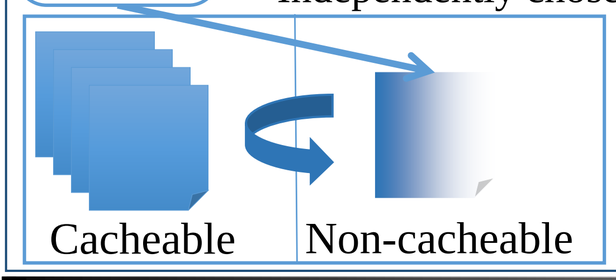
Similar reloading times with CacheBar-enable



Prime-Probe Defense

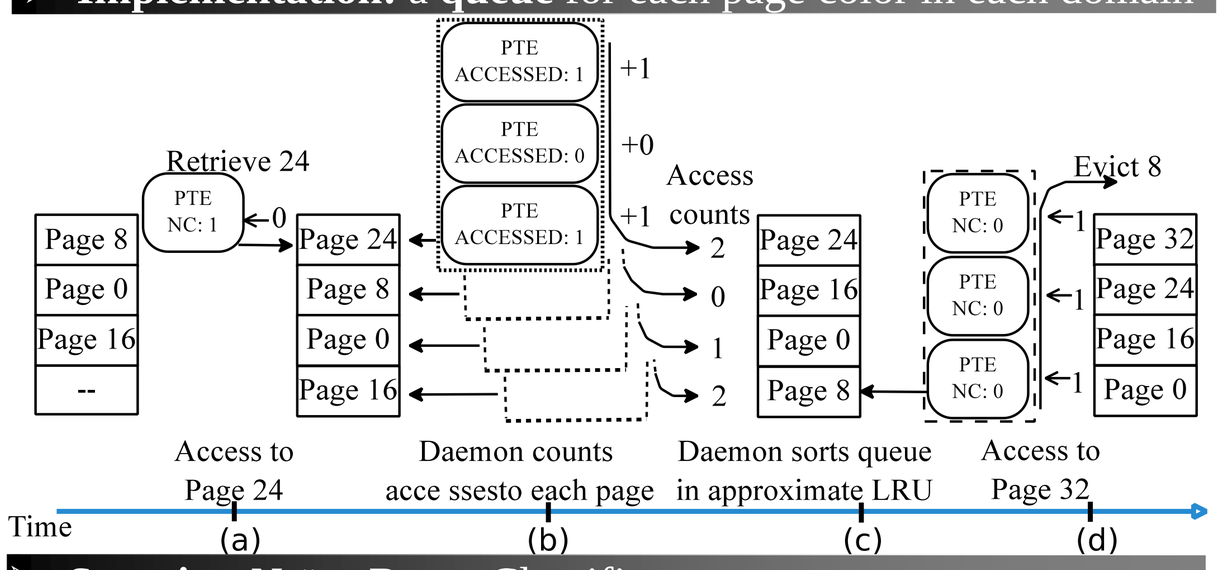
➢ Approach: Cacheable Queue

Available budget (***k***):
- ✓ < # way of LLC
- ✓ Dynamically changed
- ✓ Independently chosen



Control # of cacheable memory pages (***k***) per ***color*** and per ***domain***, to disable the ability to prime whole cache set. On access to NC page, LRU strategy is used for cacheable page replacement. In addition, three properties (✓) are used to guarantee the security.

➢ Implementation: a **queue** for each page color in each domain



➢ Security: Naïve Bayes Classifier

CacheBar-Disabled (68%)

confusion matrix		attacker's classification N	O	F	S	L	M
victim's demand	NONE	.96	.04	.00	.00	.00	.00
	ONE	.01	.80	.19	.01	.00	.00
	FEW	.00	.16	.50	.30	.04	.00
	SOME	.00	.00	.07	.54	.34	.04
	LOTS	.00	.00	.00	.03	.84	.13
	MOST	.00	.00	.00	.03	.56	.41

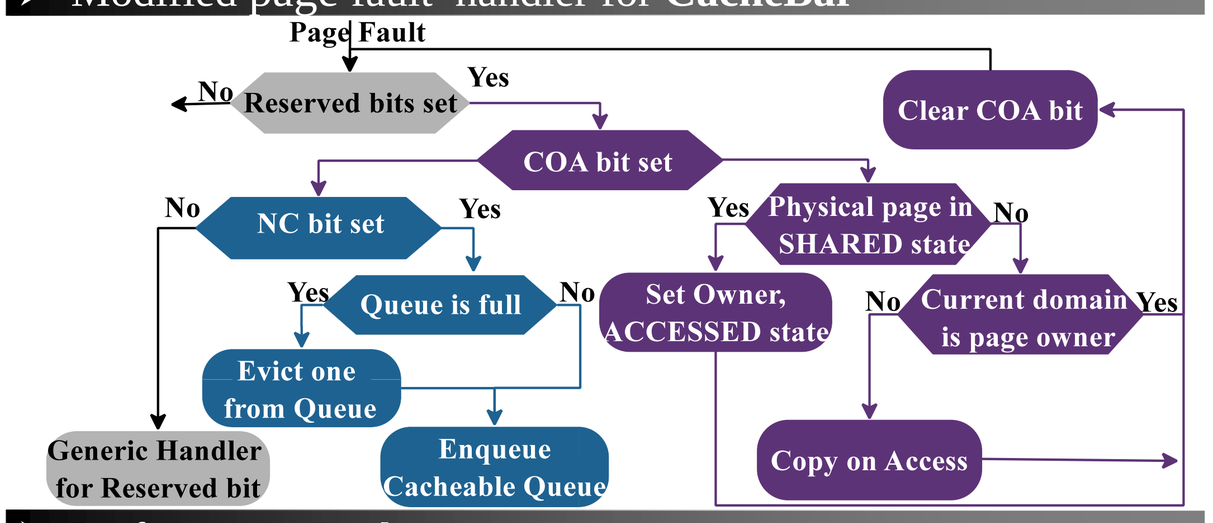
CacheBar-Enabled (33%)

confusion matrix		attacker's classification N	O	F	S	L	M
victim's demand	NONE	.34	.14	.23	.21	.06	.02
	ONE	.16	.31	.17	.23	.09	.04
	FEW	.13	.12	.34	.22	.13	.05
	SOME	.13	.10	.16	.38	.19	.05
	LOTS	.12	.08	.11	.19	.37	.12
	MOST	.14	.08	.16	.22	.18	.21

Demand ranges (way of cache=16): NONE ={0} ONE ={1} FEW ={2-4} SOME ={5-8} LOTS = {9-12} MOST = {13-16}

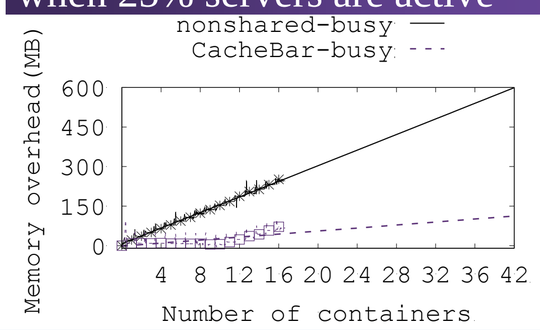
Integration

➢ Modified page fault handler for **CacheBar**



➢ Performance Evaluation

CacheBar vs. Disable sharing when 25% servers are active



Throughput for different language - webserver pairs