Security Verification of Virtual Memory Implementations with CheckMate

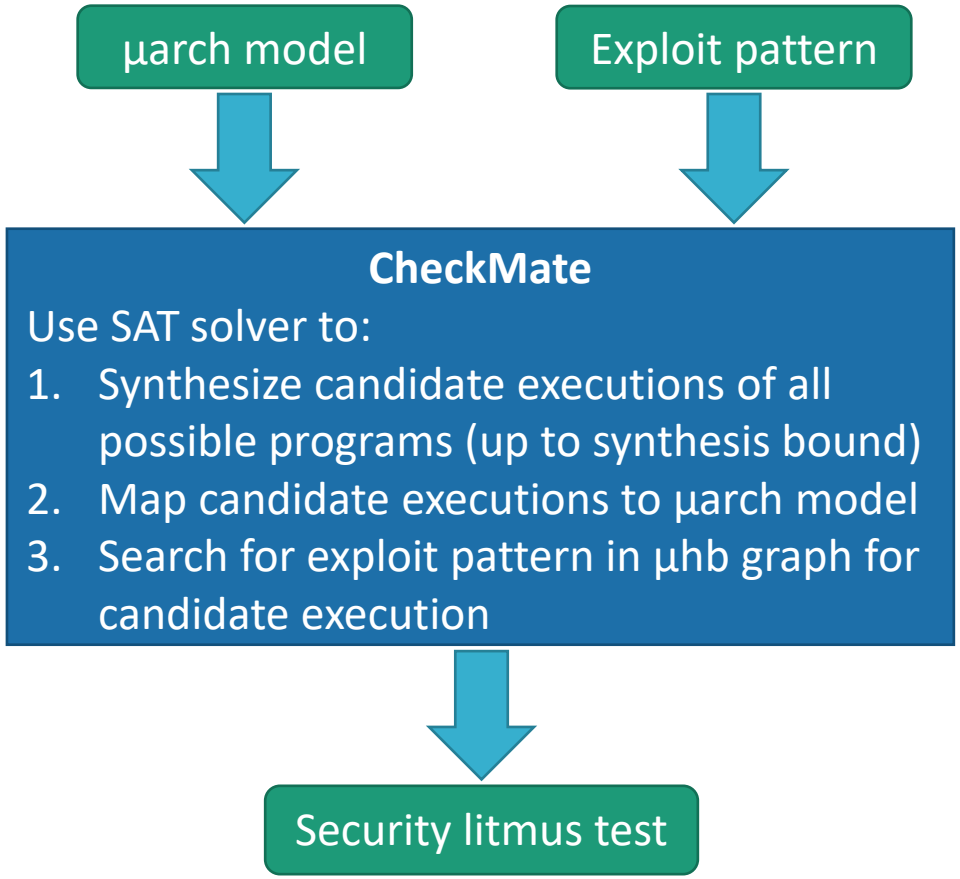
Naorin Hossain
Princeton University

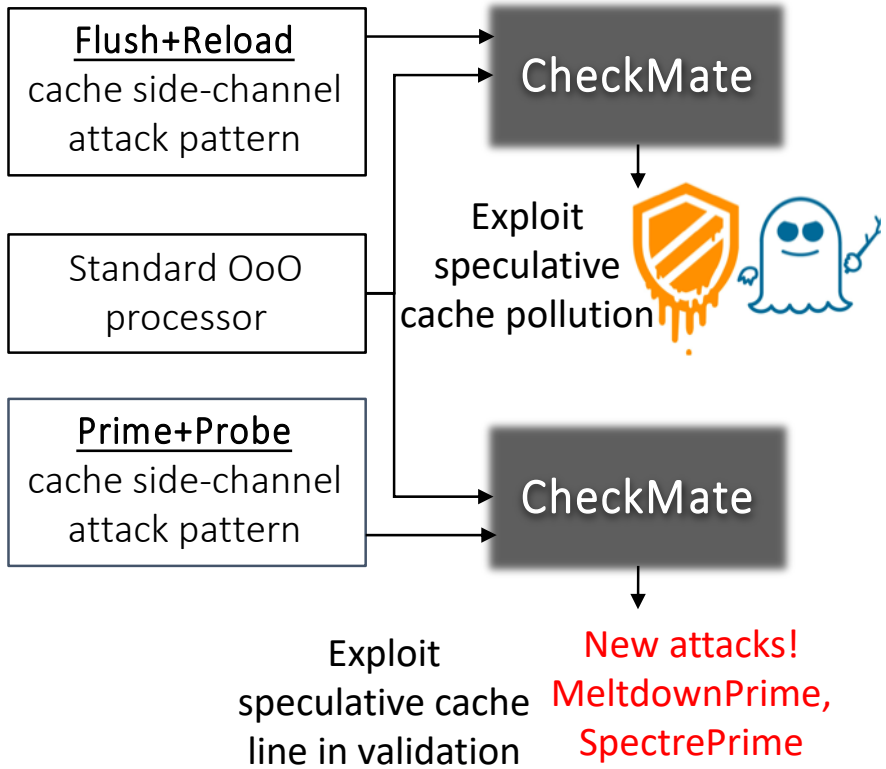
PI: Caroline Trippel
Stanford University

Intel SCAP Workshop
September 29, 2020

CheckMate: early stage verification tool for detecting hardware vulnerabilities to exploits

- Evaluates microarchitectural susceptibility to known security exploit classes and synthesizes security litmus tests for susceptible designs



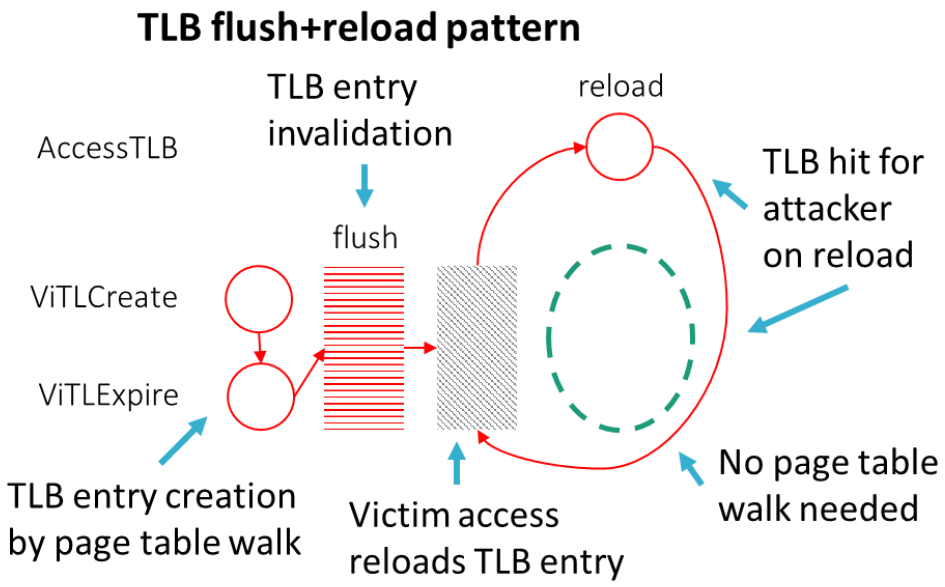


SandyBridge model: μarch model with address translation for security analysis of VM systems

Features for security analysis	Prior OoO processor model	SandyBridge model
Supported operation types	User-level operations: • Memory access • Memory fence • Branch • Cache flush	User-level operations: • Memory access • Memory fence System-level operations: • Remap V-to-P address mapping • TLB entry invalidation Hardware-level operations: • Page table walk • Dirty bit update
Structures accessible for exploits	Cache	Cache, TLB
Virtual memory assumptions	One-to-one V-to-P address mapping (no synonyms)	Synonyms permitted

SandyBridge stages

TLB flush+reload pattern synthesized on SandyBridge model



	Attacker T0 on C0	Victim T1 on C0
	(i0) R [VA1] → r2	
	(i1) ptwalk [VA0] → TLB entry1	
Flush →	(i2) INVLPG [VA1]	
		(i0) R [VA1] → r1
		(i1) ptwalk [VA0] → TLB entry2
Reload →	(i3) R [VA1] → r2