

9/18/26

COMP 435:



Computer Security Concepts

Lecture 13: Security in Practice – Hardware Side Channels



The University
of North Carolina
at Chapel Hill

<https://tinyurl.com/comp435-fa26>

Logistics Update



- First lab went out Last Friday!
 - Due Thurs 9/24
- In-Class Component of Written Assignment Due Today at 5pm!

Plan for Class Today



- 10:10-10:35 – Research together 😊
- 10:35-11:00 – Share & Synthesize

Guiding Question 😊

Can we draw any conclusions from or observe any patterns in recent hardware side-channel attacks?

Part 1



- First, spend 10-15 minutes reading, researching, taking notes on your own.
 - You can use any sources you'd like.
 - I have linked some academic papers, Wikipedia articles
 - Other acceptable resources for this exercise: blog posts, YouTube videos, asking your favorite LLM for explanations
 - 15 minutes is too short to understand everything. That is ok! We are trying to get the main ideas and key points.
- Next, 10 minutes discussing in a group!
 - Try to fill in the part 2 table for your attack.
 - Distill it down into the key points you'd like your classmates to takeaway

Part 2

- Short 3 minute presentations!
- 1 representative from each group.
2 from each attack 😊

Attack	What does it exploit?	What is the security impact?
Meltdown		
Foreshadow		
Flush+Reload / Prime+Probe		
GoFetch		
ZombieLoad		
Hertzbleed		

Meltdown



Foreshadow



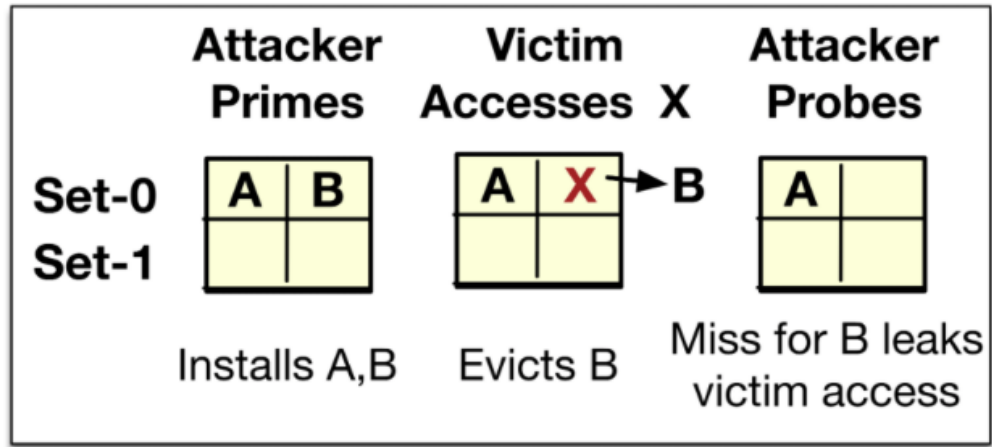
FORESHADOW

Foreshadow



FORESHADOW

Cache Attacks

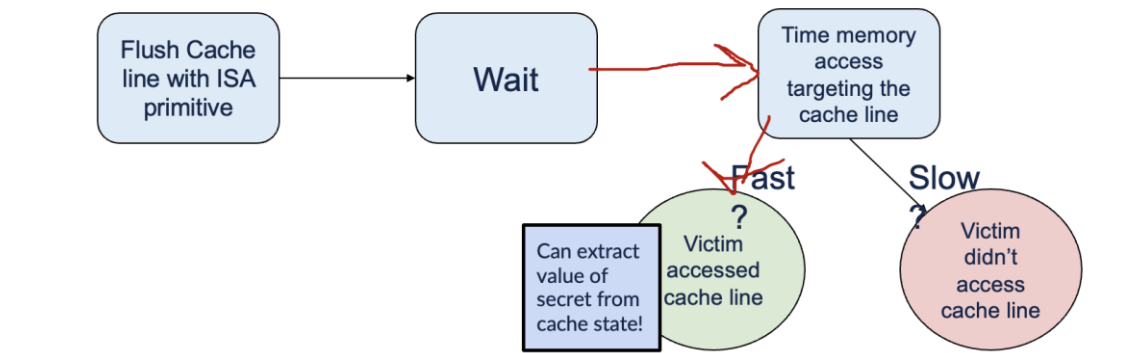


Requires
discovery of
EvictionSet (X)
= {A,B}

Lines that can
evict X

Prime+Probe Attack

Source: <https://www.sigarch.org/battle-for-secure-caches-attacks-and-defenses-on-randomized-caches/>



Flush&Reload Figure from
Lecture 11

Foreshadow



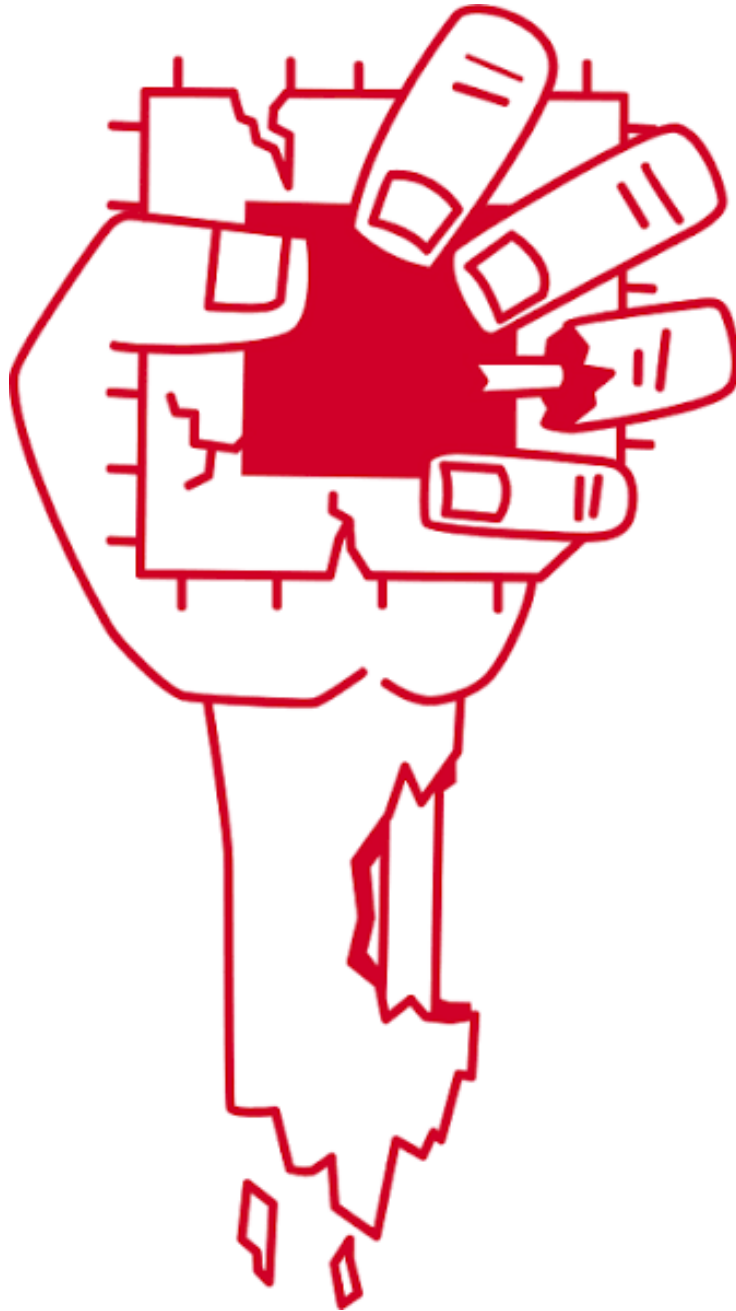
FORESHADOW

GoFetch



GoFetch

ZombieLoad



HertzBleed



Hertzbleed

Patterns I noticed 😊



- A hardware optimization or implementation detail creates an observable effect that violates an assumption made by software.
- Information can leak through hardware behavior even when the attacker cannot directly access the protected data.