

9/16/26

COMP 435:

Computer Security Concepts



Lecture 12: Rowhammer Attacks



The University
of North Carolina
at Chapel Hill

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

Logistics Update



- First lab went out Friday!
 - Due Thurs 9/24
- 2nd Written Assignment due Thursday at 11:59pm.
 - In-class component 70%. Work in small groups to trace a real side-channel attack from start to finish
 - Pre-class component 30%. I passed out Monday!

More Details About Friday



- Work in small groups to investigate a real hardware or side-channel attack
- Use credible sources to figure out:
 - What the attacker is trying to learn or control
 - What hardware behavior or side channel is exploited
 - What the attacker can observe
 - How the attack turns that observation into useful information
- Connect the attack back to our class concepts:
 - cache state
 - timing
 - speculation
 - information flow
- Prepare a short group explanation to share with the class
 - I will assign topics day before.
- Complete an in-class worksheet summarizing your findings

Plan for Class Today



- 10:10-10:15 – Accept the lab!!
- 10:45-11:00 – Rowhammer Guest Lecture!

Guiding Question 😊

How can an attacker tamper with memory without directly accessing it!?!?