Lecture 24: Memory, Security

- Today’s topics:
  - Main memory system
  - Hardware security intro
Off-Chip DRAM Main Memory

• Main memory is stored in DRAM cells that have much higher storage density

• DRAM cells lose their state over time – must be refreshed periodically, hence the name *Dynamic*

• A number of DRAM chips are aggregated on a DIMM to provide high capacity – a DIMM is a module that plugs into a bus on the motherboard

• DRAM access suffers from long access time and high energy overhead
- DIMM: a PCB with DRAM chips on the back and front
- The memory system is itself organized into ranks and banks; each bank can process a transaction in parallel
- Each bank has a row buffer that retains the last row touched in a bank (it’s like a cache in the memory system that exploits spatial locality) (row buffer hits have a lower latency than a row buffer miss)
Hardware Security

• Software security: key management, buffer overflow, etc.
• Hardware security: hardware-enforced permission checks, authentication/encryption, etc.
• Security vs. Privacy
• Information leakage, side channels, timing channels
• Meltdown, Spectre, SGX
Meltdown
Spectre: Variant 1

\[
\begin{align*}
\text{Victim Code:} & \quad \text{if} \ (x < \text{array1\_size}) \\
& \quad y = \text{array2}[\ \text{array1}[x]]; \\
\end{align*}
\]

- \(x\) is controlled by attacker
- Thanks to bpred, \(x\) can be anything
- array1[ ] is the secret
- Access pattern of array2[ ] betrays the secret
Spectre: Variant 2

Attacker code

Label0: if (1)

Label1: ...

Victim code

R1 ← (from attacker)
R2 ← some secret
Label0: if (...)

... ...

Victim code

Label1:

lw [R2]