CA : HW8.

1. Security.

Spectre	Meltdown
→ They are not caused by any bug in the hardware design.	→ It's caused by hardware design oversight by Intel.
→ This attack tricks processors or victim code to execute instructions they shouldn't ~~have~~ and hence getting access to sensitive / secret data in other application's memory	→ This attack simply runs the attacker code in the system to access sensitive data that it shouldn't have access to.
→ Branch prediction & extreme speculation helps this attack to gain access to other application's memory.	→ Speculative nature of processors results in leaving footprints of sensitive data which the attacker doesn't have permission to access like passwords.
→ To fix this kind of attack, we can partition the cache so that attacker can't access other applications' memory, but this not an efficient fix.	→ To fix this kind of attack, we shouldn't allow the speculations to proceed and leave footprints once we know that the instruction doesn't have the permission to.

2. Snooping-Based Cache

Req.	Cache hit/ miss	Req. on bus	who responds	C1 state Inv	C2 state Inv	C3 state Inv
P1: Wr X	Write Miss	Wr X	Memory	M	Inv	Inv
P2: Rd X	Read Miss	Rd X	P1 responds, Memory Writeback	S	S	Inv
P1: Rd X	Read Hit	-	-	S	S	Inv
P2: Wr X	Perm Miss	Upgrade X	No response, other caches invalidate.	Inv	M	Inv
P3: Wr X	Write Miss	Wr X	P2 responds	Inv	Inv	M
P3: Rd Y	Read Miss	Rd Y	Memory, Memory Writeback	Inv	Inv	S
P2: Wr Y	Write Miss	Wr Y	memory, other caches invalidate	Inv	M	Inv
P1: Rd Y	Read Miss	Rd Y	P2 responds, Memory Writeback	S	S	Inv

while implementing Write invalidate protocol, there are 4 interconnect message transfers.

3. Directory-Based cache coherence

Req	Cache hit/ Miss	Messages	Dir	C1	C2	C3	C4
				I	I	I	I
P1: Wr X	Write miss	Wr-req to Dir. Dir responds.	X : M : 1	M	I	I	I
P2: Rd X	Read miss.	Rd-req to Dir. Dir forwards req to P1. P1 sends data to Dir. Memory Writeback. Dir sends data to P2.	X : S : 1,2	S	S	I	I
P1: Rd X	Read Hit	–	–	S	S	I	I
P2: Wr X	Perms miss	Upgrade req to Dir. Dir sends Inv to P1, P1 sends ACK to Dir. Dir grants perms to P2.	X : M : 2	I	M	I	I
P3: Wr X	Write miss	Wr-req to Dir. Dir forwards req to P2. P2 sends data to Dir. Dir sends data to P3.	X : M : 3	I	I	M	I
P3: Rd Y	Read miss	Rd-req to Dir. Memory Writeback. Dir responds.	Y : S : 3	I	I	S	I
P2: Wr Y	Write miss	Wr-req to Dir. Dir sends INV to P3. P3 sends ACK to Dir. Dir sends data and permission to P2.	Y : M : 2	I	M	I	I
P1: Rd Y	Read miss.	Rd-req to Dir. Dir forwards req to P2. P2 sends data to Dir Memory Writeback. Dir sends data to P1.	Y : S : 1,2	S	S	I	I