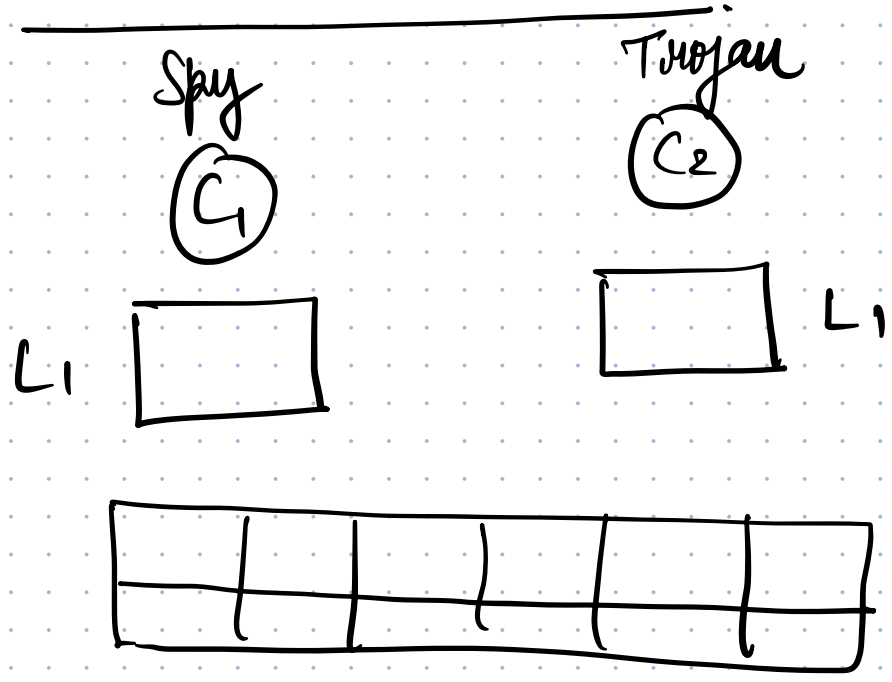
Types of attacks:

→ Covert channel attacks (CCA): 2 attack appli

→ Side channel attacks (SCA): only 1 attack appli

Covert channel Attack (CCA):



→ Trojan has to send some info to spy.

→ The info is sequence of binary.

→ The trojan and spy should have way to convey 0 and 1.

Types of covert channel attacks:

→ Prime + Probe attacks

→ Flush + Reload attacks

* Eviction set: The set of address used by the spy and

trojan. Typically belonging to the same set.
To carry out attacks.

Prime + Probe: Prime → Wait → Probe

Prime phase
→ Create eviction sets for spy and trojan.
→ Spy will request the eviction set.
→ This would replace the set with known eviction set.

Wait phase:
→ Spy will wait.
→ Trojan wants to communicate
↳ Bit 0: ⇒ Do nothing
↳ Bit 1: Request its own eviction set.
Since the eviction sets of spy & trojan, the trojan would replace the spy's block.

Probe phase:

→ Bit 0 ⇒ All hit

→ Bit 1 ⇒ All miss for spy

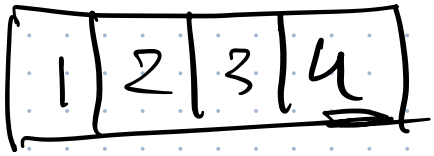
The time difference is used to understand the miss

(Eg.) Spy eviction set: A B C D

Trojan eviction set: 1 2 3 4

Prime

Wait:



Probe:

Less Time for fetch → Bit 0

More time for fetch → Bit 1

Flush + Reload attack: Flush → Wait → Reload.

Assumption: Trojan & Spy have the same eviction set.

Flush phase:

→ Flush set with non-evict set

Wait:

→ Bit 0: Trojan does nothing

→ Bit 1: Trojan request for eviction set.

Reload:

→ Spy will request for eviction set

→ All miss → Bit 0

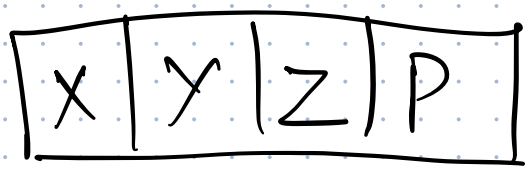
→ All hit → Bit 1

} Based on time difference.

(Eg) Eviction set of spy & trojan

A B C D

Flush:



Wait:

Reload:

Fetch ABCL

Add miss
↓
More time to fetch
↓
Bit 0

Add hit
↓
Less time to fetch
↓
Bit 1