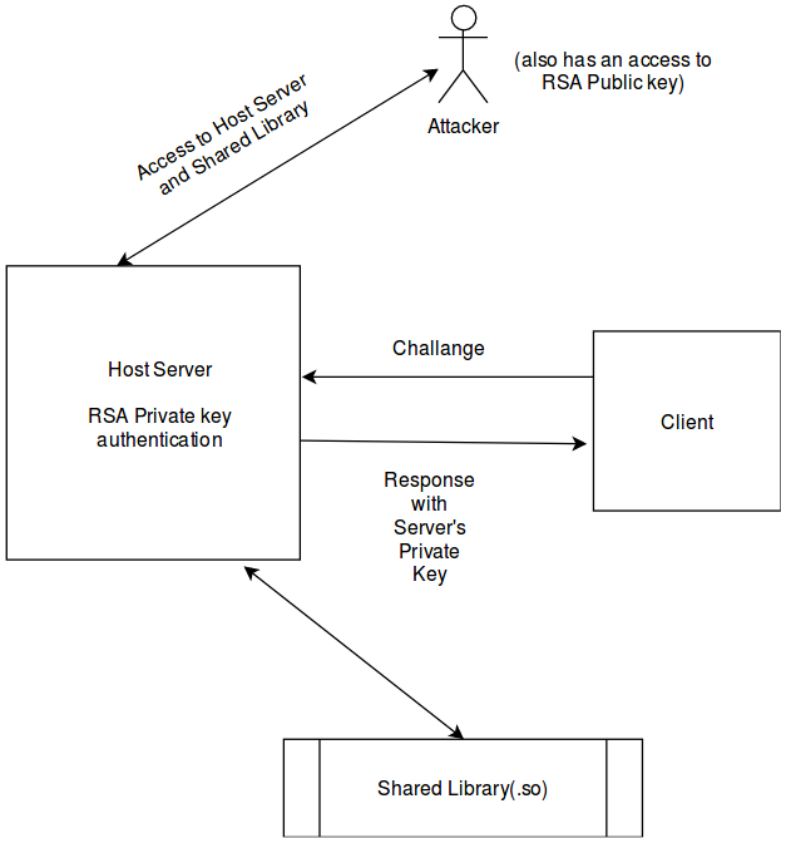
Part 4 - RSA private key extraction

Given scenario



The attacker has gained access to the Host server and the shared library , that has code to generate the RSA Private Key. However , the public key is known to the attacker. Following are the cases where we discuss how the Cache side channel attack can be useful in extracting the Private Key.

- What memory locations (code or data) could be used in Flush and Reload cache side channel attack ?

–- The attacker applies FLUSH and RELOAD technique within victim's **Code Segment**. This will help an attacker to place probes within victim program that will be executed as well, whenever the victim executes the code in probed memory lines. By this way an attacker can spy and infer the internal state of the victim's program and trace the execution.

- How could you determine the Private Key based on the cache timing measurements ?

–- An attacker can trace the execution of the square ,multiply and modulo-reduce calculations to recover the exponent. To do so , it should divide the time into

slots of respective CPU cycles , and in each slot it should probe one memory line of the code of each operation sequence. After probing the memory lines , an attacker flushes lines from the cache and waits till end of the time slot.

Attacker then measures the time to read the memory lines in each operation , also read those lines when are brought into cache and read by the attacker.

- What difficulties could arise that might make the attack fail in practice ?

1) Access control enforcements on clflush instruction
2) If an attacker to miss the time slots resulting bit it errors in capturing the sequences
3) Noise created by running multiple processes in the background
4) Spy and victim are not on the same physical processor

- How could the attacker verify the extracted private key is correct ?

— When the attacker has an Private Key (d,n), he can get exponent 'e' from that further , he can get the public key (e,n) from the same. He then can verify the same with Public key which is already known to him. If both public keys are same the he can be sure that , extracted private key is correct.