Cache timing attacks

To get started

- A timing attack is a side channel attack in which the attacker attempts to compromise a cryptosystem by analyzing the time taken to execute cryptographic algorithms.
- Known to be practical against RSA, ElGamal, and the Digital Signature Algorithm.
- The DSA algorithm works in the framework of public-key cryptosystems and is based on the algebraic properties of the modular exponentiations, together with the discrete logarithm problem.

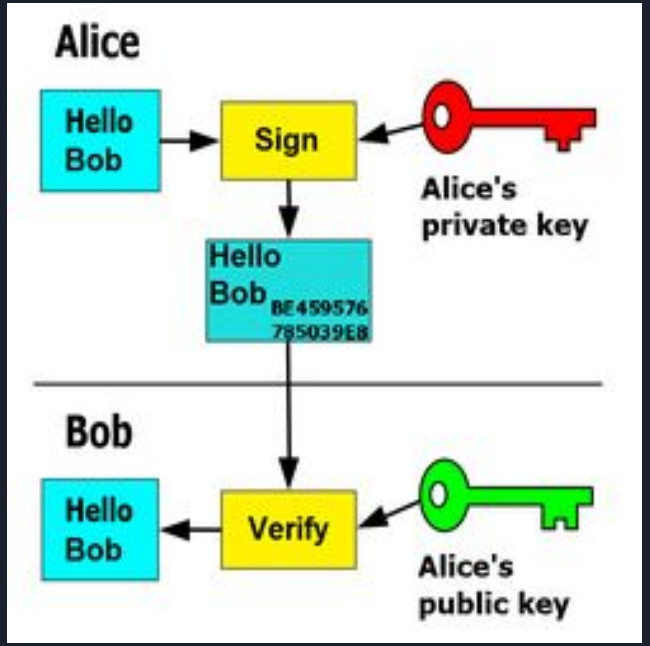
About DSA

Used to sign messages

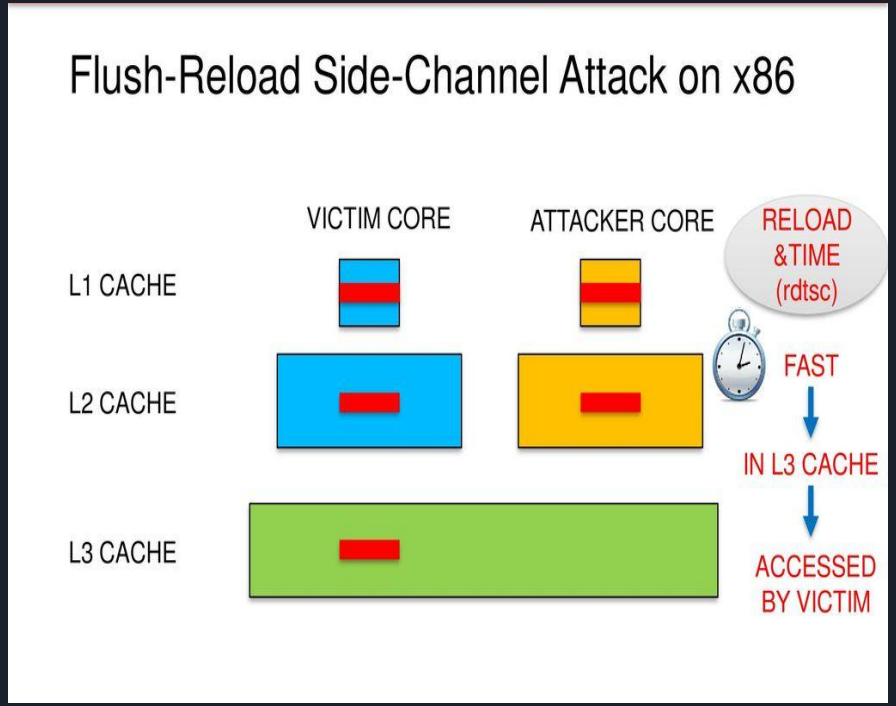
Acknowledge ownership

Protection based on discrete logarithm

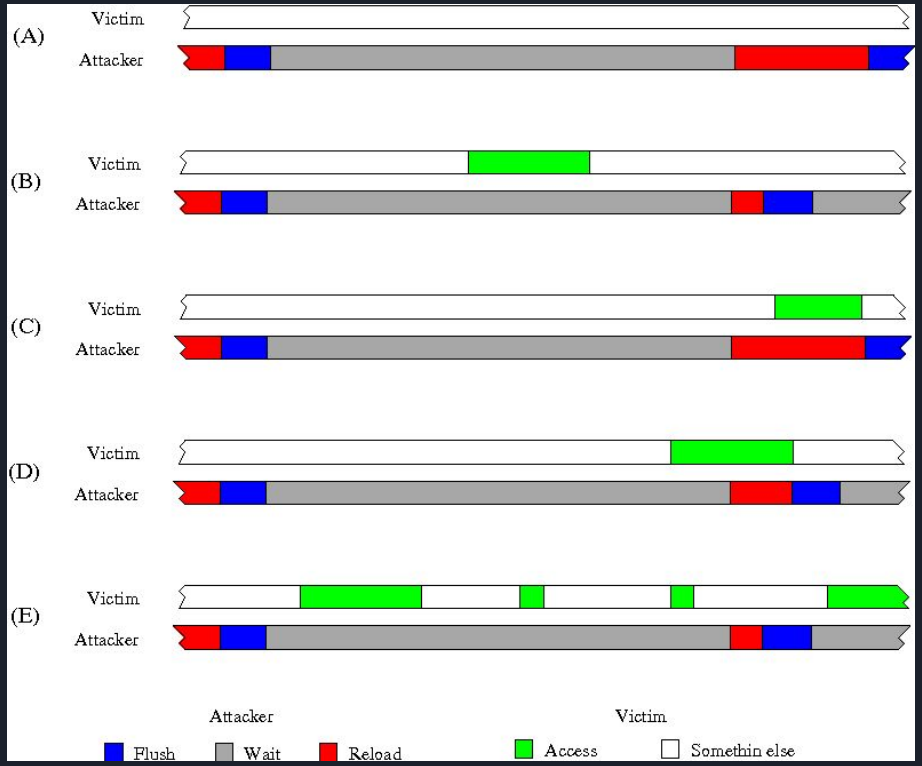
In practice, FLUSH+RELOAD can be used to get the key while modular exponentiation



FLUSH+RELOAD



FLUSH+RELOAD



FLUSH+RELOAD Example

With Modular Exponentiation

```
x ⟵ 1
for i ⟵ |e|-1 downto 0 do
    x ⟵ x² mod n
    if (e_i = 1) then
        x = xb mod n
    endif
done
return x
```

Implementation

Found some open-source tools implementing FR attacks

Simple victim program takes a binary number as an input and branches if the number is 1

Spy program to check if number input is 1

Cache Techniques

EVICT+TIME

Trigger victim to encrypt a chosen plaintext C

Evict selective lines from cache

Again invoke victim to encrypt C

PRIME+PROBE

Fill up (prime) the cache with attacker's data

Allow victim to run

Probe the cache contents

FLUSH+RELOAD

Flush a particular line

Allow victim to run

Access that particular line