UNIVERSITY OF **DAMASCUS**

Start

What is side channel attacks

Types of attacks based on the side channel

Countermeasures

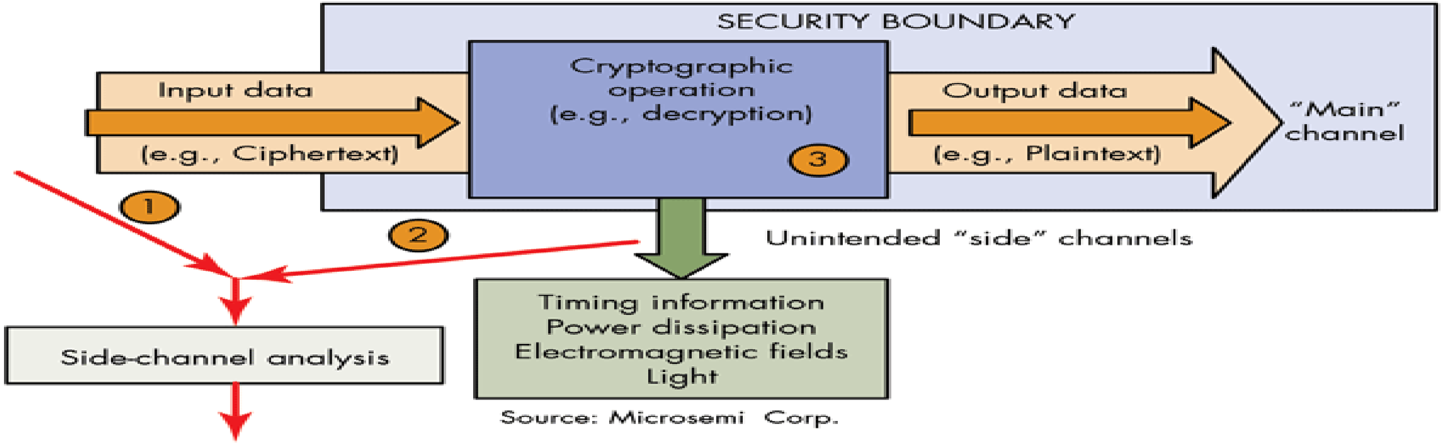
SIDE CHANNEL ATTACKS IN CLOUD COMPUTING

عدي الخزاعي
محمد لؤي العش
معاذ العجلاني
محمد علي العقال

What is Side channel attacks?

What is Side channel??

* Side-channel attacks aim to retrieve secret data from a cryptographic system by observing factors outside the normal computation.



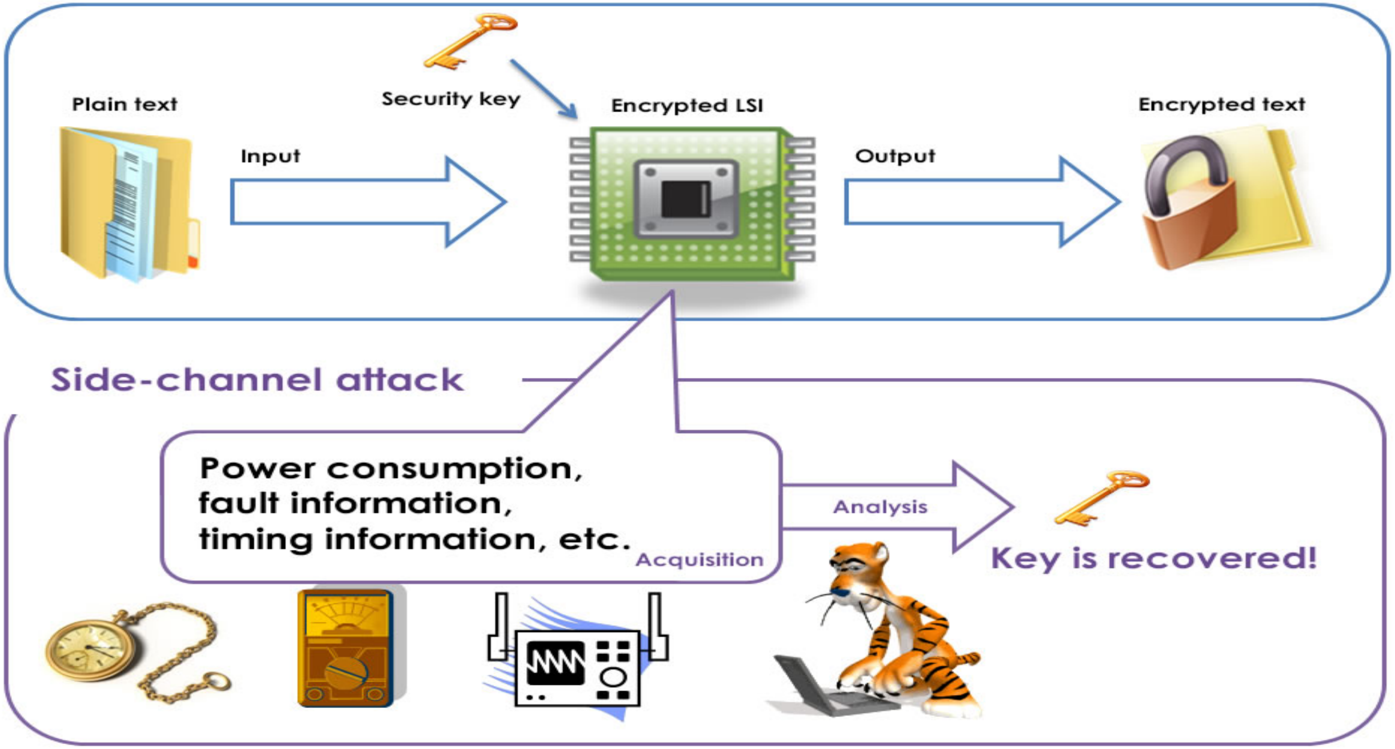
Source: Microsemi Corp.

* While it is good to have a system that is mathematically secure, this alone does not tell the whole story. There are attacks that aim not at the mathematical properties of the cryptographic system, but at implementation,hardware, electromagnetic radiation, timing and even sound. can provide an extra source of information, which can be exploited to break the system

Types of attacks based on the side channel

Types of attacks based on the side channel

- attacks that target power consumption
- attacks that target timing
- attacks that target faulty



Types of attacks based on the side channel

Power analysis

* Power analysis attacks are based on the notion that power consumption of cryptographic hardware is not constant during execution

1. Simple Power Analysis
2. Differential Power Analysis

Simple Power Analysis

* With simple power analysis, we can attempt to retrieve information directly from the power consumption of the device.

* such that any conditional branches that depend on secret data potentially leak information about that data

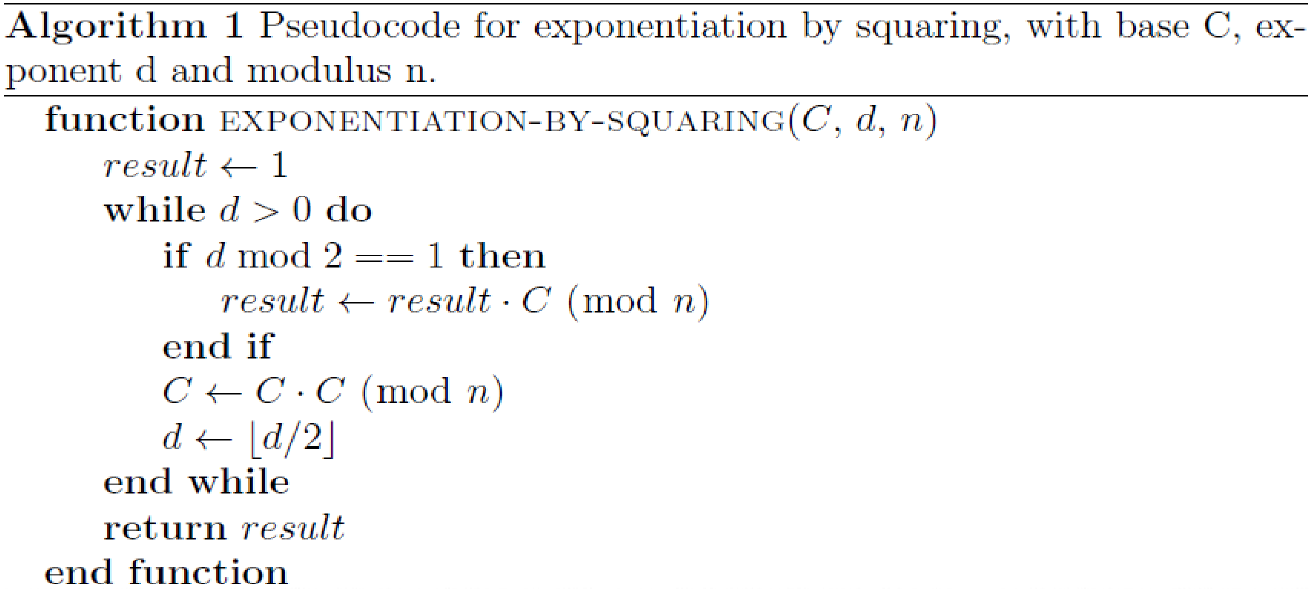
* A common example used for illustration is the RSA public-key cryptography system . In RSA, decryption is performed by exponentiation of the ciphertext with the secret key.

A fast and straightforward
way to do this is by employing exponentiation by squaring

Types of attacks based on the side channel

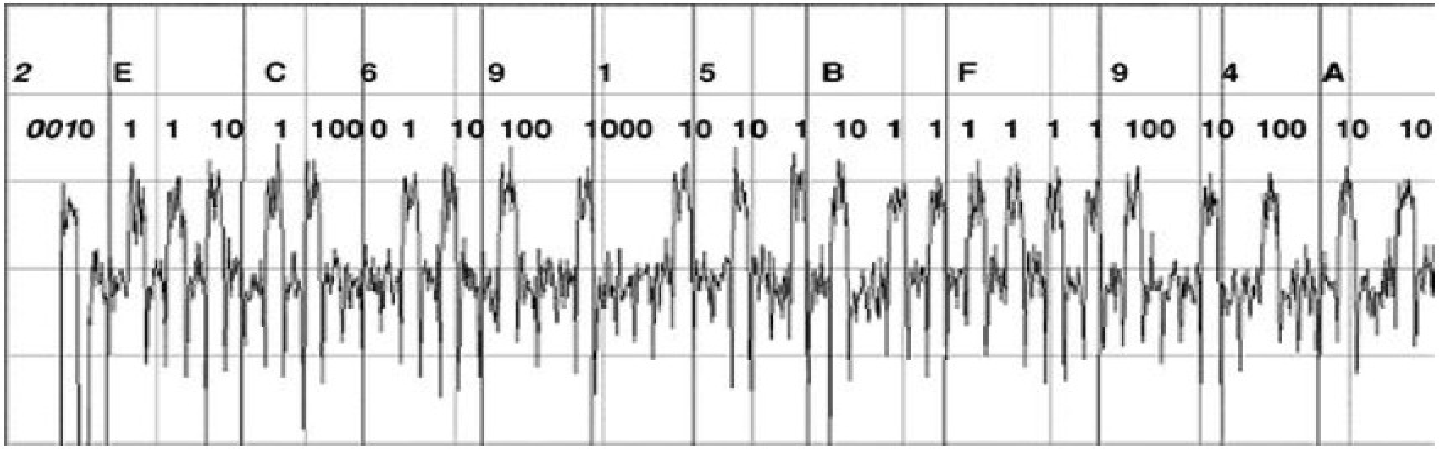
Power analysis

Simple Power Analysis



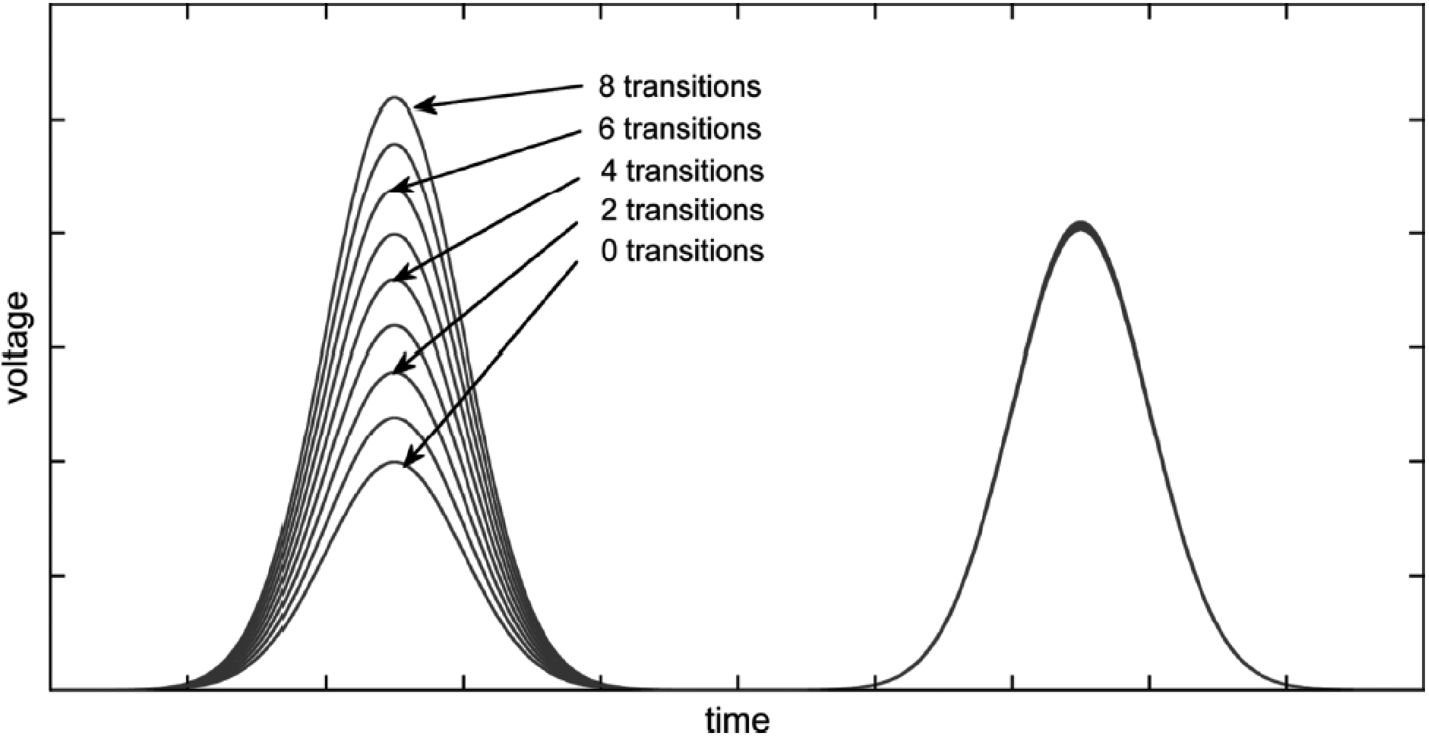
Algorithm 1 Pseudocode for exponentiation by squaring, with base C, exponent d and modulus n.

```
function EXPONENTIATION-BY-SQUARING($C$, $d$, $n$)
    $result \leftarrow 1$
    while $d > 0$ do
        if $d \bmod 2 == 1$ then
            $result \leftarrow result \cdot C \pmod{n}$
        end if
        $C \leftarrow C \cdot C \pmod{n}$
        $d \leftarrow \lfloor d/2 \rfloor$
    end while
    return $result$
end function
```



Differential Power Analysis

* Simple power analysis works well on cryptographic algorithms that have a strong correlation between the values of secret data and the power consumption of the hardware. Such a strong correlation is, however, not always present. In many such cases, differential power analysis can be of use



Countermeasures

For the case of simple power analysis, it is generally enough to ensure no conditional branches depend on secret data. For instance, one can prevent simple power analysis on RSA decryption as mentioned above by adding dummy operations that ensure all code paths perform the same computations. Alternatively, one can employ a different method of exponentiation, called the Montgommery Powering Ladder

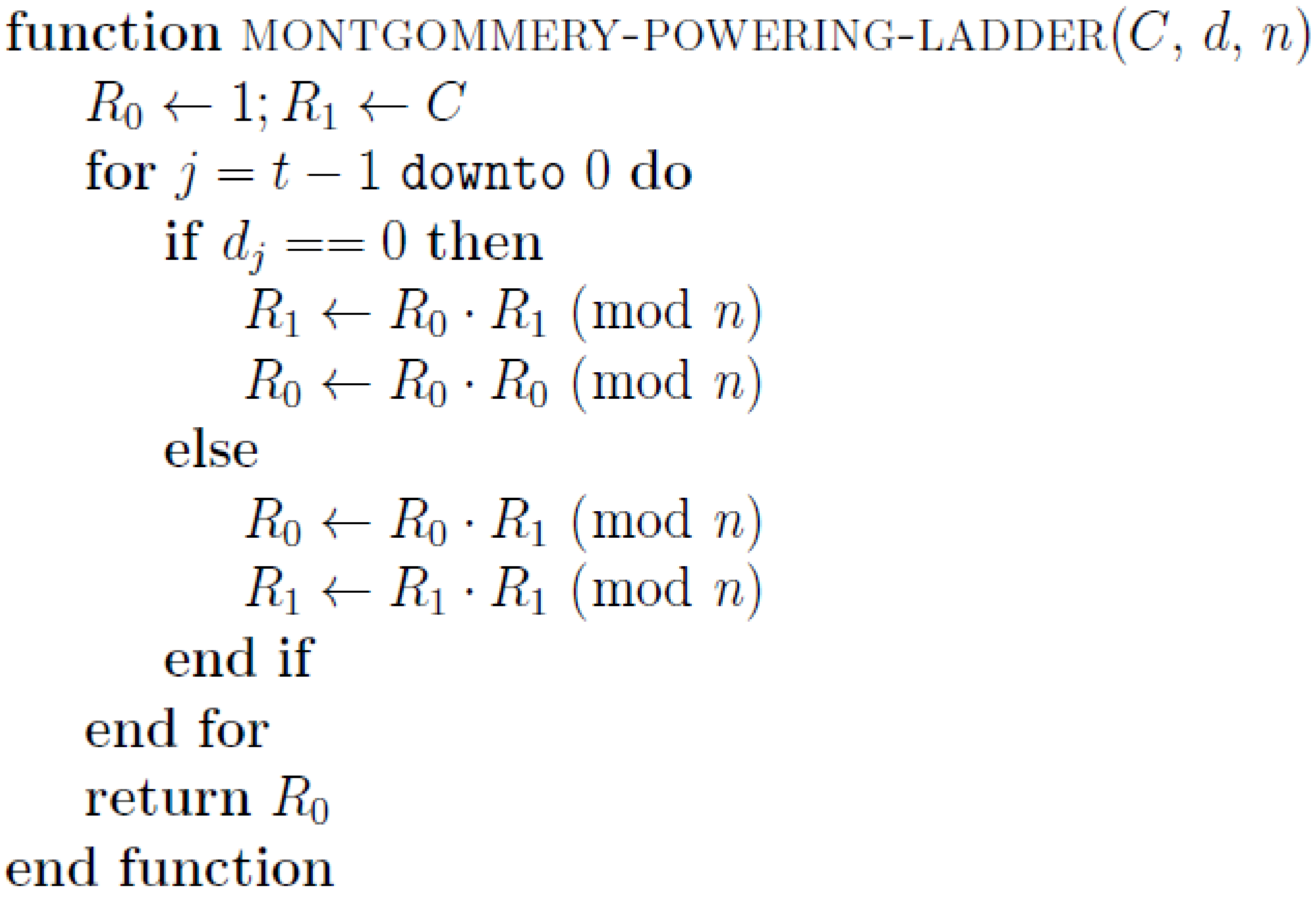
Types of attacks based on the side channel

Power analysis

Countermeasures

Countermeasures

Pseudocode for the Montgommery Powering Ladder, with base C, exponent d and modulus n. dj is the j^th bit of d.



```
function MONTGOMMERY-POWERING-LADDER($C$, $d$, $n$)
    $R_0 \leftarrow 1; R_1 \leftarrow C$
    for $j = t - 1$ downto $0$ do
        if $d_j == 0$ then
            $R_1 \leftarrow R_0 \cdot R_1 \pmod{n}$
            $R_0 \leftarrow R_0 \cdot R_0 \pmod{n}$
        else
            $R_0 \leftarrow R_0 \cdot R_1 \pmod{n}$
            $R_1 \leftarrow R_1 \cdot R_1 \pmod{n}$
        end if
    end for
    return $R_0$
end function
```

Countermeasures

Preventing differential power analysis is more complicated. For public-key algorithms, it is possible to blind the secret data

This paper aims at presenting a new countermeasure against Side-Channel Analysis (SCA) attacks, whose implementation is based on a hardware-software co-design. The hardware architecture consists of a microprocessor, which executes the algorithm using a false key, and a coprocessor that performs several operations that are necessary to retrieve the original text that was encrypted with the real key. The coprocessor hardly affects the power consumption of the device, so that any classical attack based on such power consumption would reveal a false key. Additionally, as the operations carried out by the coprocessor are performed in parallel with the microprocessor, the execution time devoted for encrypting a specific text is not affected by the proposed countermeasure. In order to verify the correctness of our proposal, the system was implemented on a Virtex 5 FPGA. Different SCA attacks were performed on several functions of AES algorithm. Experimental results show in all cases that the system is effectively protected by revealing a false encryption key.

Types of attacks based on the side channel

Timing

Timing

1- Conventional timing attacks

Secret Data ↔ Time taken to perform a computation in order to retrieve the Secret Data

he-timing :

ng attack aims to recover secret data by monitoring

1- Conventional timing attacks

Example: RSA Decryption $E(x) = x^d \bmod n$

```
function exponentiation-by-squaring(C, d, n)
    result ← 1
    while d > 0 do
        if d mod 2 == 1
            result ← result · C (mod n)

        C ← C · C (mod n)
        d ← bd/2c

    return result
```

Types of attacks based on the side channel

Timing

Conventional timing attacks

How to Attack?

1- Conventional timing attacks

How To Attack?

.....Samples!!!

How much Time?
How many Samples???

Types of attacks based on the side channel

Timing

Conventional timing attacks

How to Attack?

Countermeasures

1- Conventional timing attacks

Countermeasures:

Noise addition: adding Dummy computations

Constant Time Execution

Force All crypto operations to take the same time

Performance ~ Confidentiality

Types of attacks based on the side channel

Timing

Cache Timing

2- Cache Timing

Recover Secret Data by monitoring cache performance

2- Cache Timing

Statistically get the key by comparing with timing calculated in advance for some know keys

Types of attacks based on the side channel

Timing

Cache Timing

How to Attack?

2- Cache Timing

Flush And Reload

Types of attacks based on the side channel

Timing

Cache Timing

How to Attack?

Countermeasures

2- Cache Timing

Countermeasures

Disallow cache altogether

No cache sharing

Redesign the cache

Random permutation cache

Types of attacks based on the side channel

timing

Countermeasures

Countermeasures

* For conventional timing attacks, it is recommended to employ blinding . This way, any data leaked reveals nothing about the secret key.

* To prevent cache-timing attacks suggest to redesign the current method of caching, proposing a random permutation cache, which randomises the cache allocation so as to not reveal which parts of the cache correspond to what data. It is worth noting that hardware implementations of cryptographic algorithms generally lack any form of caching, meaning that only software implementations meant for general-purpose computers are vulnerable to this type of attack

Types of attacks based on the side channel

Fault analysis

Fault analysis

Fault analysis

* Fault analysis attacks attempt to retrieve secret data from the result of faulty computations.

* These computations may come about through faulty hardware or deliberate tampering with the device or software.

Types of attacks based on the side channel

Fault analysis

Fault analysis

Conventional fault analysis :

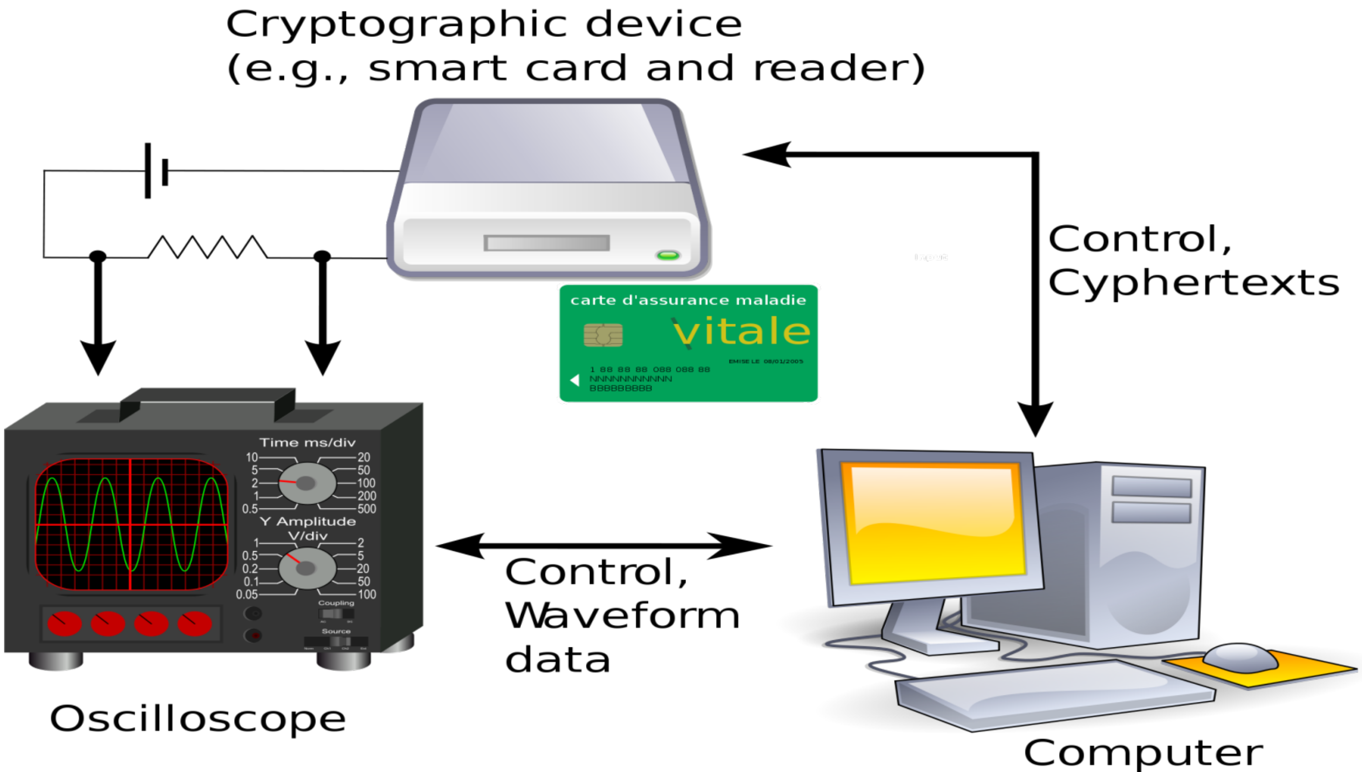
Conventional fault analysis aims to retrieve secret data by analysing the result of faulty encryptions

Differential fault analysis :

Some researchers expand on the notion of fault analysis, making it applicable to symmetric cryptographic systems as well. They call their approach differential fault analysis. Their attack works under the assumption that it is possible to induce a fault in the computation at some random point.

Countermeasures

* One way of defending against fault analysis attacks is to check the result of the cryptographic function before outputting it.



Side Channel attack in Cloud Computing

What is Cloud ?

Cloud Computing

Resources on the internet

Advantages: shared resources is cost effictive

Disadvantages: Users' Security

- Shared resources → Information Leakage?

rackspace HOSTING

Dropbox

NETFLIX

amazon webservices™

Google docs

Windows Azure

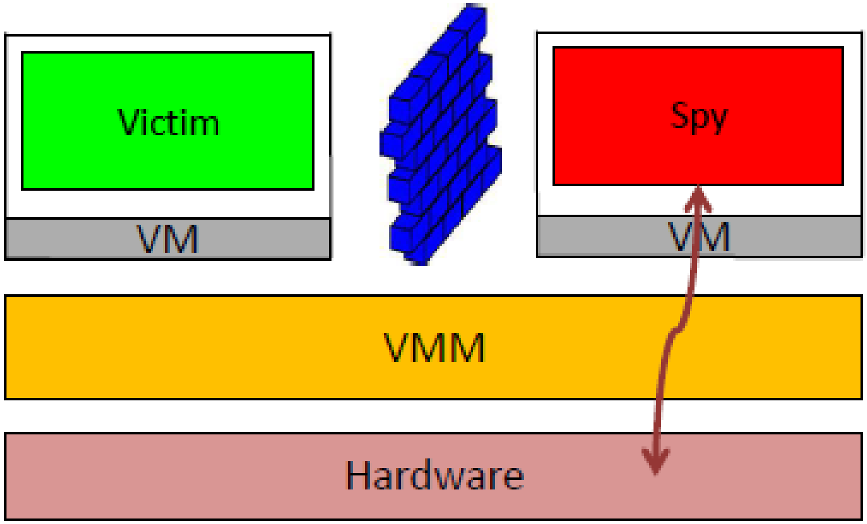
Virtual Machines

Multi-tenancy in Cloud

- One machine for many clients

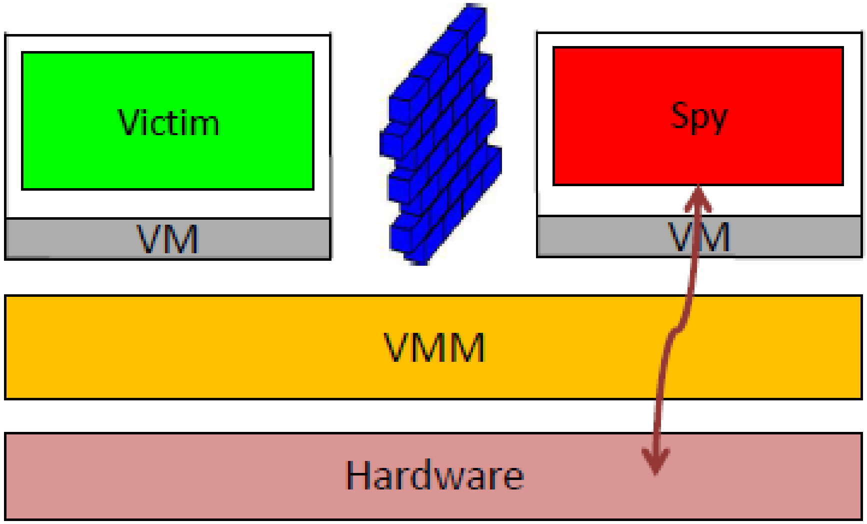
Problem

- Shared Cache



How To Attack?

The attacker place his virtual machine as a co-resident machine in the cloud environment



Side Channel attack in Cloud Computing

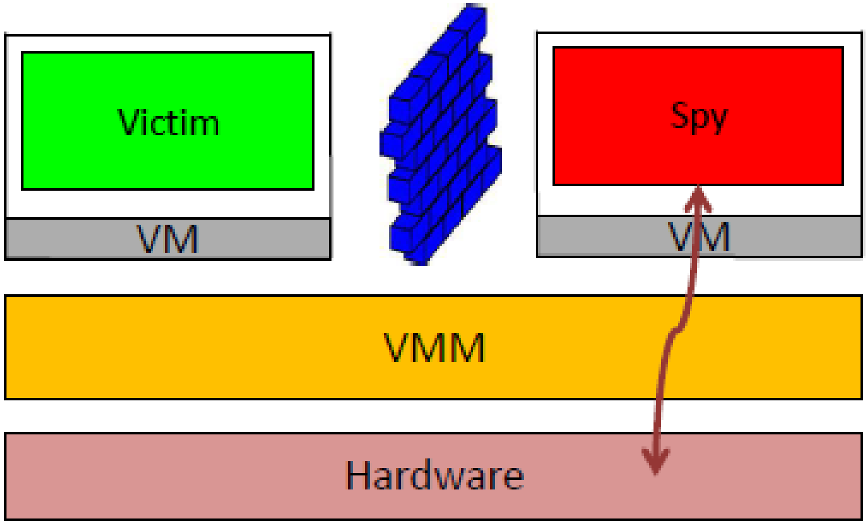
What is Cloud ?

Virtual Machine

How to attack?

How To Attack?

The attacker place his virtual machine as a co-resident machine in the cloud environment



Side Channel attack in Cloud Computing

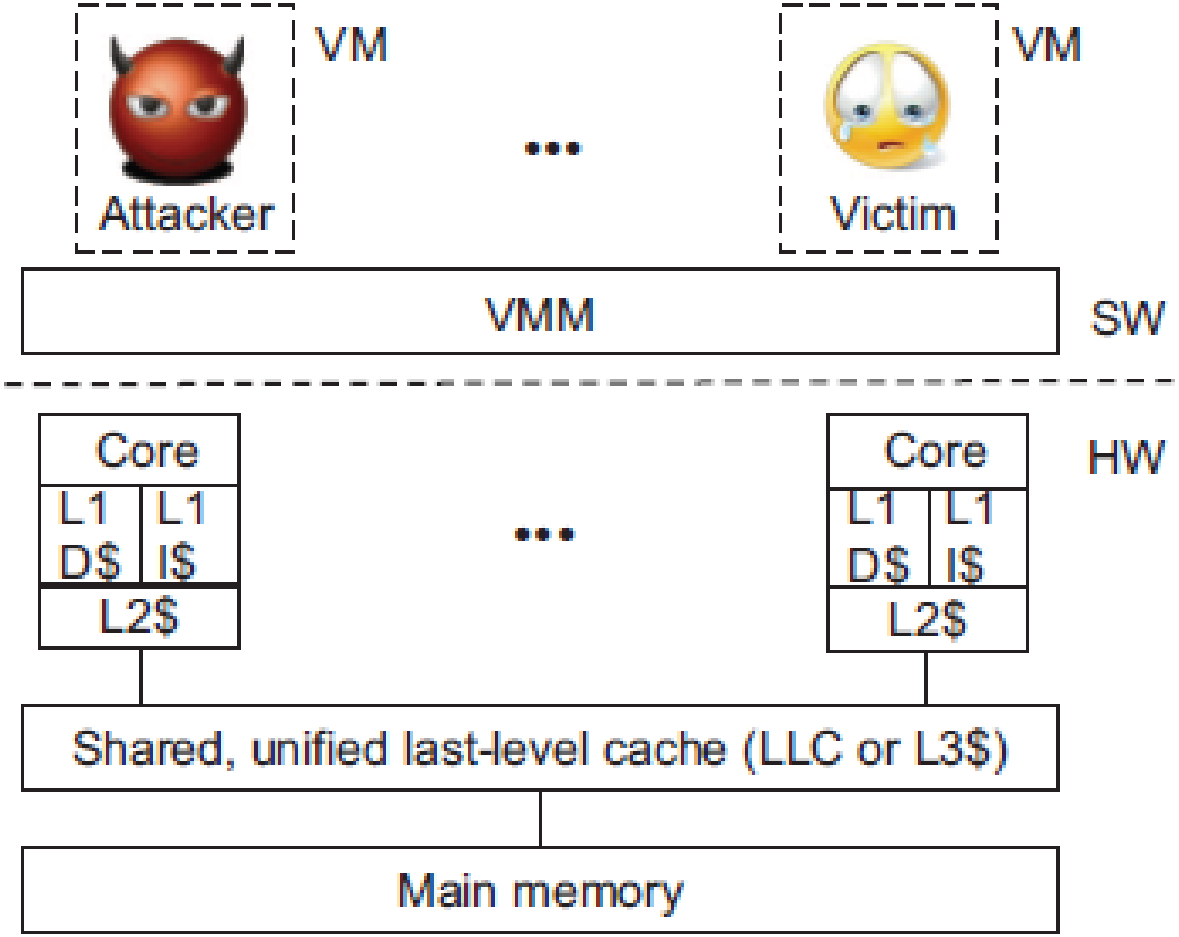
What is Cloud ?

Virtual Machine

How to attack?

Cache-based side channel attack

Cache-based side channel attack



Side Channel attack in Cloud Computing

What is Cloud ?

Virtual Machine

How to attack?

Cache-based side channel attack

Types

Types

Side Channel attack in Cloud Computing

What is Cloud ?

Virtual Machine

How to attack?

Cache-based side channel attack

Types

Access-driven attack

Access-driven attack

Prime and probe

Flush and reload

Side Channel attack in Cloud Computing

What is Cloud ?

Virtual Machine

How to attack?

Cache-based side channel attack

Types

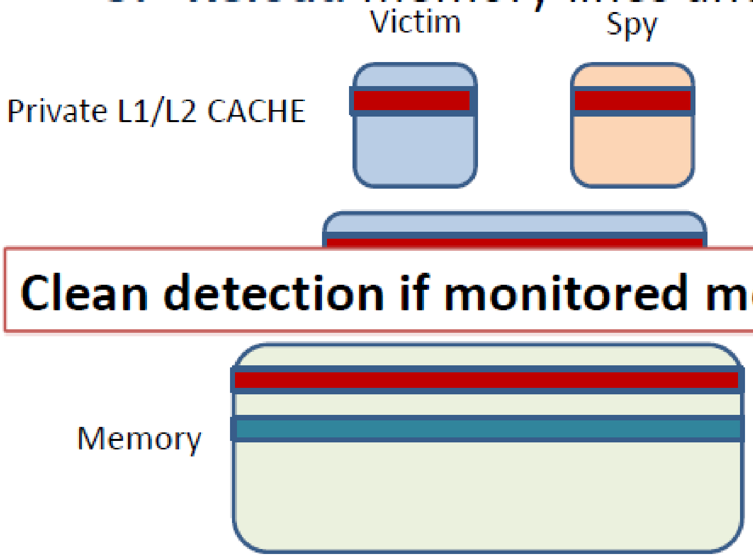
Access-driven attack

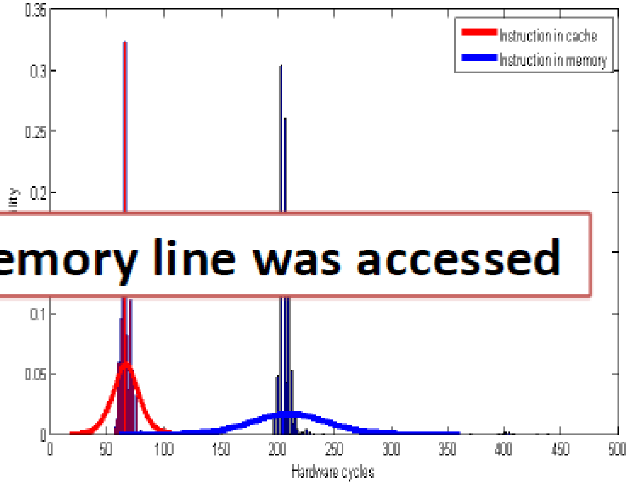
Flush and reload

Flush and reload

Steps:

1. **Flush** desired memory lines
2. Wait for some time
3. **Reload** memory lines and measure reload time.





Clean detection if monitored memory line was accessed

security

Side Channel attack in Cloud Computing

What is Cloud ?

Virtual Machine

How to attack?

Cache-based side channel attack

Types

Access-driven attack

Flush and reload

Trace-driven attack

Trace-driven attack

References

- CloudRadar: A Real-Time Side-Channel Attack Detection System in Clouds

http://link.springer.com/chapter/10.1007%2F978-3-319-45719-2_6

- Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing

http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper19.pdf

- Defending against cache-based side-channel attacks

http://ac.els-cdn.com/S1363412703001043/1-s2.0-S1363412703001043-main.pdf?_tid=faf09d24-9084-11e6-be2500000aacb35d&acdnat=1476281330_c4a212c4cadc07504d1d939c6d55
e01

References

Thanks!

Thanks !!