Side Channel Attacks

...

Concept

- Electronic circuits leak information.
- A side-channel attack is based on information that is obtained from such leaks.
- These leaks do not play a part in the operation of the circuit itself, they are simply side effects of the circuit working.
- A side-channel attack does not focus on weaknesses in the implemented system.
- Side-channel attacks monitor power consumption, timing and acoustic information, heat, electromagnetic emissions, and others.

DNS Cache Poisoning

DNS

- It’s an hierarchical distribution of servers that communicate with each other through the hierarchy to resolve queries.
- It allows the users to know a name instead of an IP, which is easier to remember.
- Before DNS there was a central entity that had a registry of all the information.

DNS Cache Poisoning

Let’s see a demonstration...

We will show:

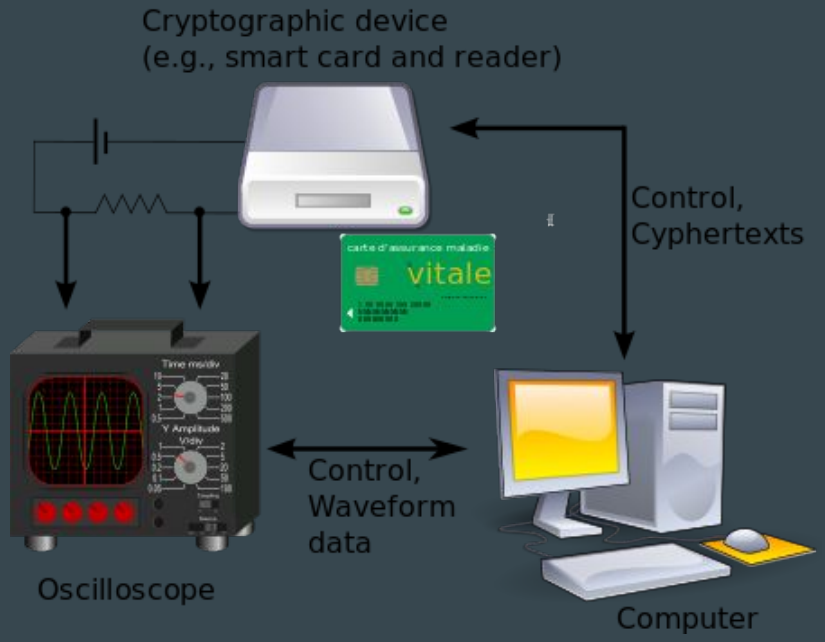
- our own implementation;
- an implementation of other authors.

Data Remanence

- To extract information from storage devices its owner thought it didn’t exist.
- Upon deletion of a file/folder, the index is removed from the Master File Table.
- TRIM command allows an OS to inform an SSD which memory areas can be wiped.

Power Analysis vs RSA

- Analyzing the power consumption of a cryptographic device.
- C^D mod N = M, where C is the encoded message received, D the private key, N is part of the public key and M is the original message.

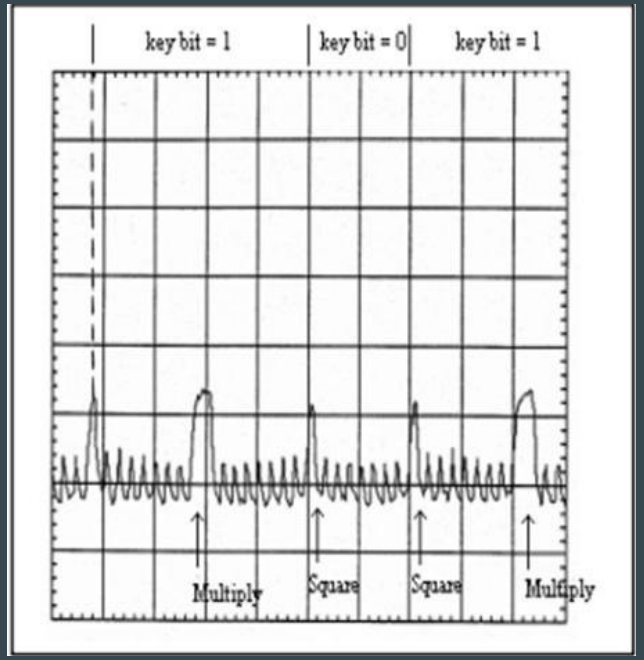


Power Analysis vs RSA

Square and Multiply

```
public static long square_multiply(long base, long power){
        long result = 1;
        while(power > 0) {
                if(power%2 == 1) {     //Special condition
                        result = result * base;
                }
                base = (long) Math.pow(base, 2);
                power /= 2;
        }

        return result;
}
```



Row Hammer Attack

To remember...


8GB 2RX8 PC4-2133P-SBB-11
Product of CHINA


Seagate
Barracuda
1000GB


intel
4th Gen
Intel® Core™ i7

To remember...

- CPU tries to switch between different running applications.
- While trying to switch, it stores part of what is doing in internal memory (DRAM).

Meanwhile...

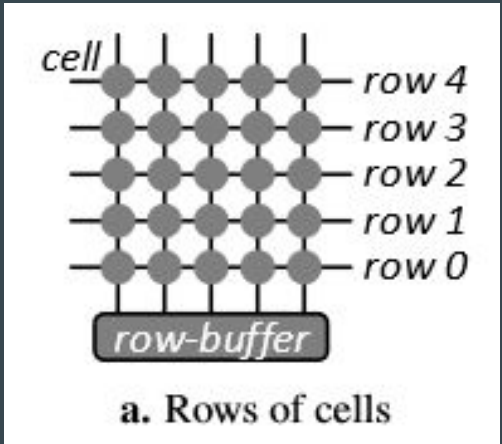
- The Operating System is doing the same thing. It stores its code and data in the DRAM.

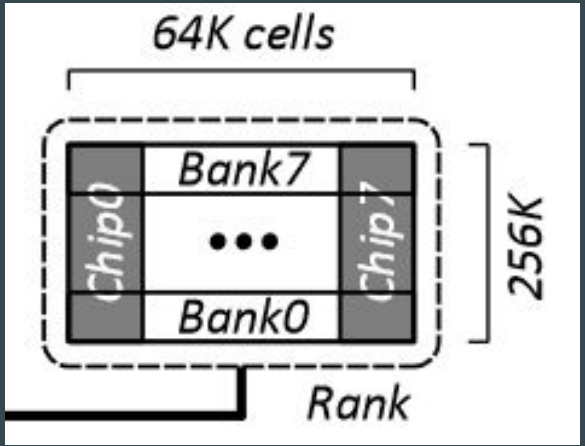
As a consequence....

- Data gets interleaved.

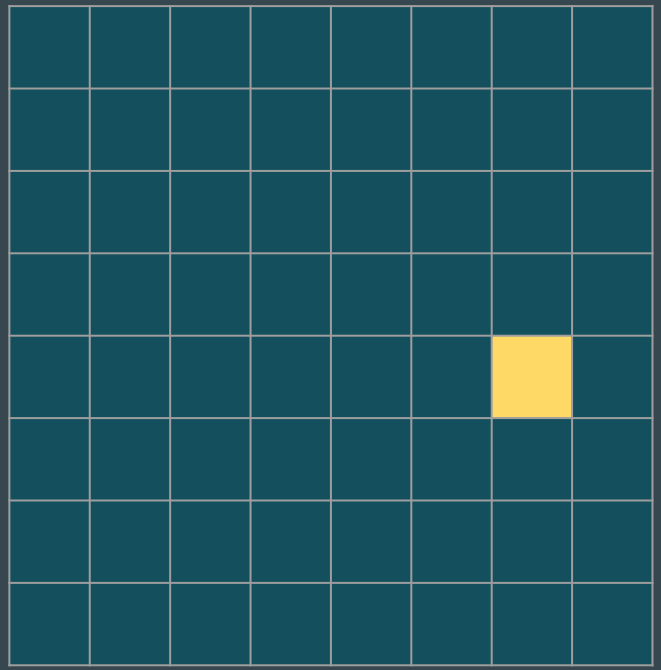
What is DRAM?

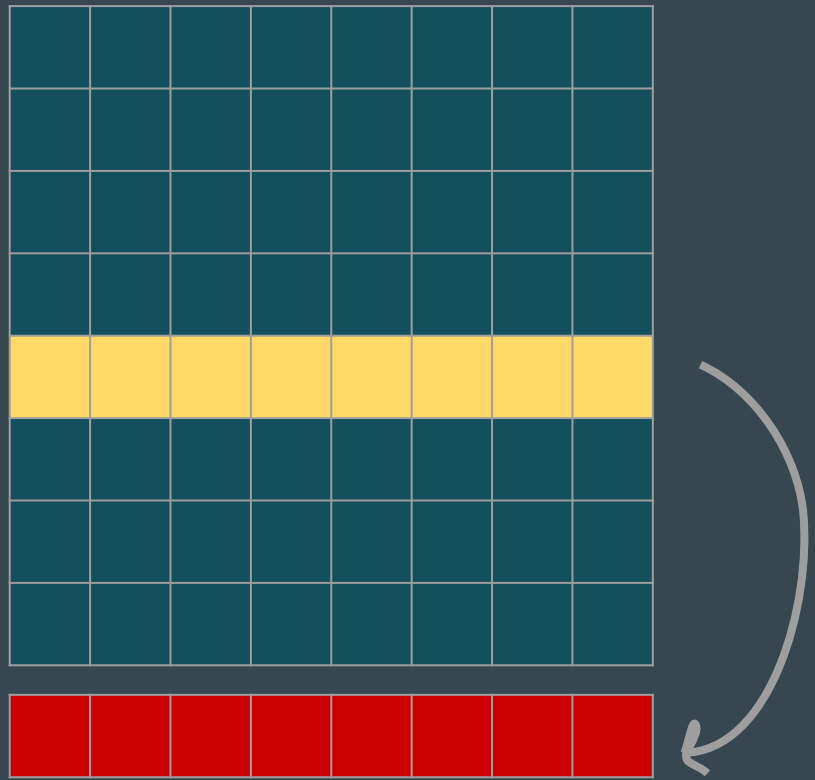
- It is a type of random access memory (RAM) where each bit of stored data occupies a separate memory cell.
- Memory cells are implemented with one capacitor and one transistor.
- The capacitor can either be charged (1) or discharged (0).





Accessing a bit of data....





DRAM data is not persistent...

- The electric charge in memory cell's capacitor start to leak off
- Data needs to be refreshed

When?

- Periodically
- After a read operation

Why?

- To prevent data loss
- To prevent data corruption

Problem...

“Memory isolation is a key property of a reliable and secure computing system—an access to one memory address should not have unintended side effects on data stored in other addresses.”

- Manufacturers started to place memory cells closer to each other.

Advantages...

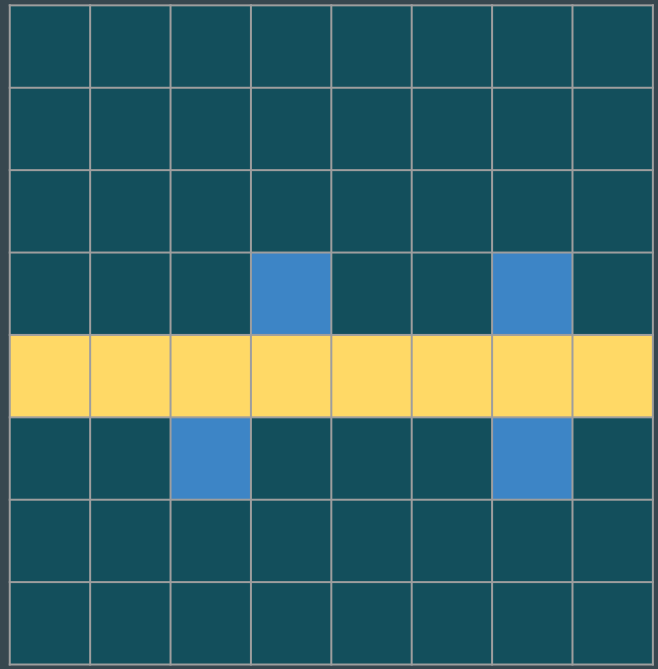
- Reduced the cost-per-bit of memory.

Disadvantages...

- Cells started to interact electrically with each other in undesirable ways, causing charge to leak into or out of neighboring cells.

Row Hammer...

- Repeatedly accessing one (or two) different memory locations...
- ... cells adjacent to the row may have their values changed...
- ... if their values are not refreshed before losing too much charge.



How to prevent...

- Use error correcting code (ECC).
- Refresh rows more frequently.
- Refresh adjacent rows when a row is accessed.
- Apply “buffer” rows to the process.
- Others.