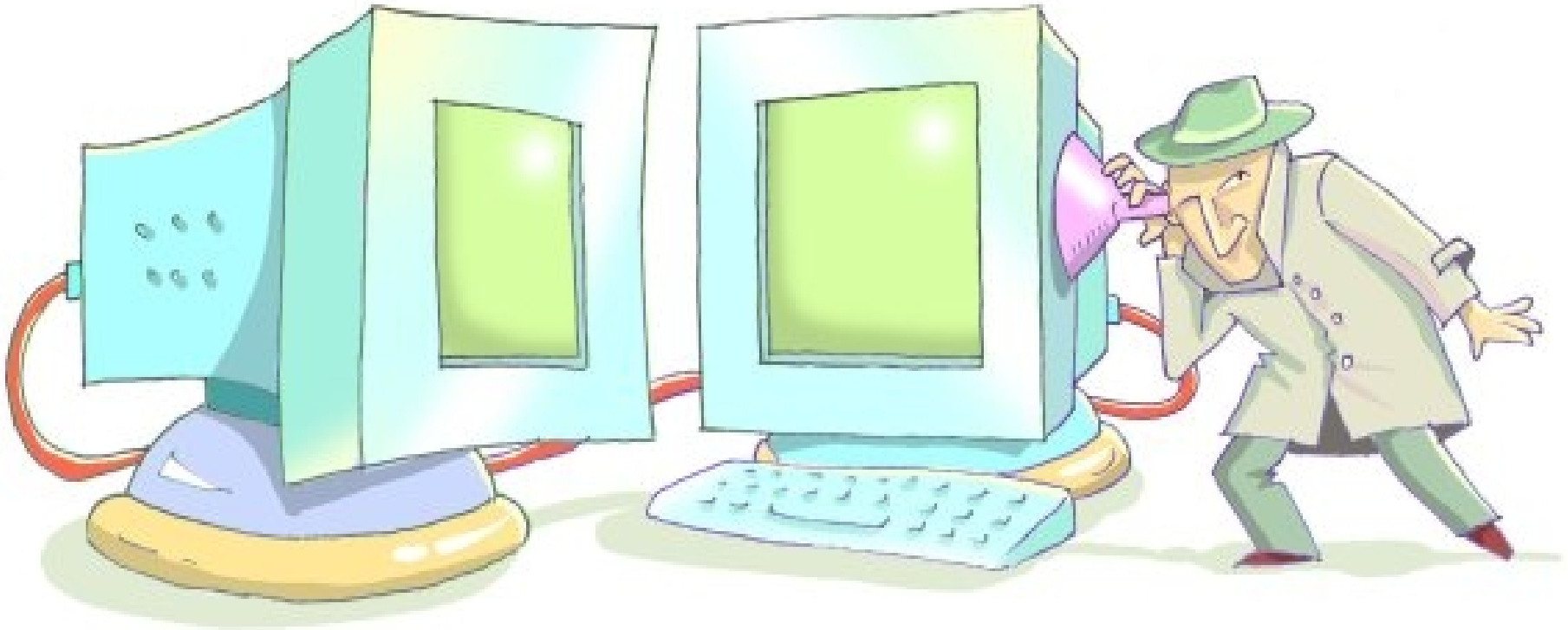
Side-Channel Attacks



Oop !!! Who am I ??

- Name : Tien Phan
- Nick : Crazyboy
- From:
  - http://bkitsec.vn
  - http://wargame.vn

- Bio : I’m a guy, who interested in hacking
- Email : moc.liamg@ti.traeh2traeh

Contents :

1. Introduction
2. Side channel attacks on web
3. Conclusions
4. Q&A

Introduction to side channel attacks

Introduction to side channel attacks

Side channels

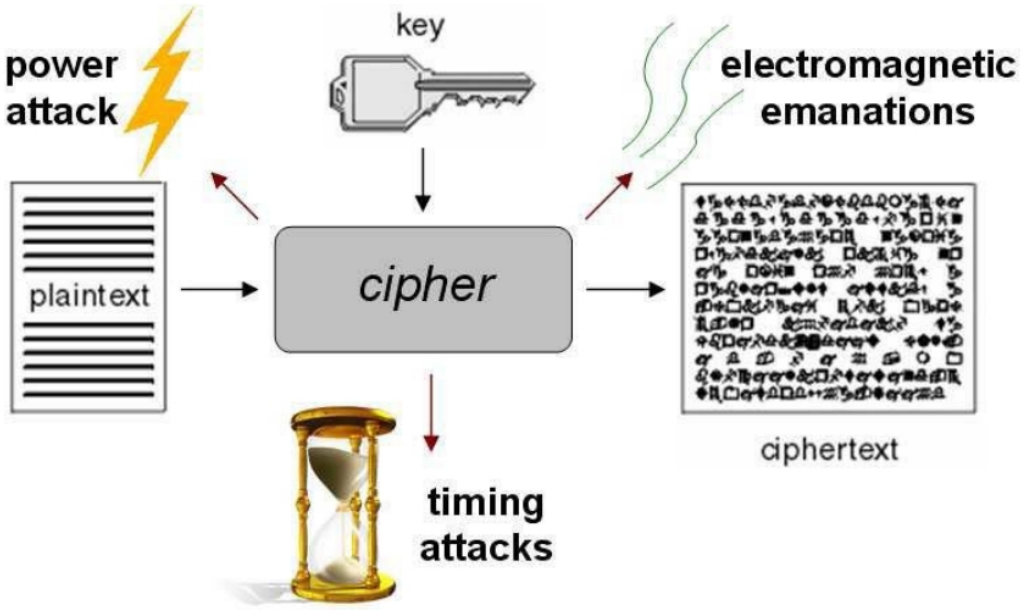
- Information leakage from implementation
  - Example: safecracker feels tumblers impacting and opens lock without trying each combination

  - Similarly: in cryptanalysis, hacker observes time/power and cracks cipher without trying each key
- Device in normal operation, no physical harm

Examples

Example side-channels on a desktop computer:

- Time
- Heat
- Noise
- Cache contents
- Electromagnetic
- Power consumption



Side channel attacks

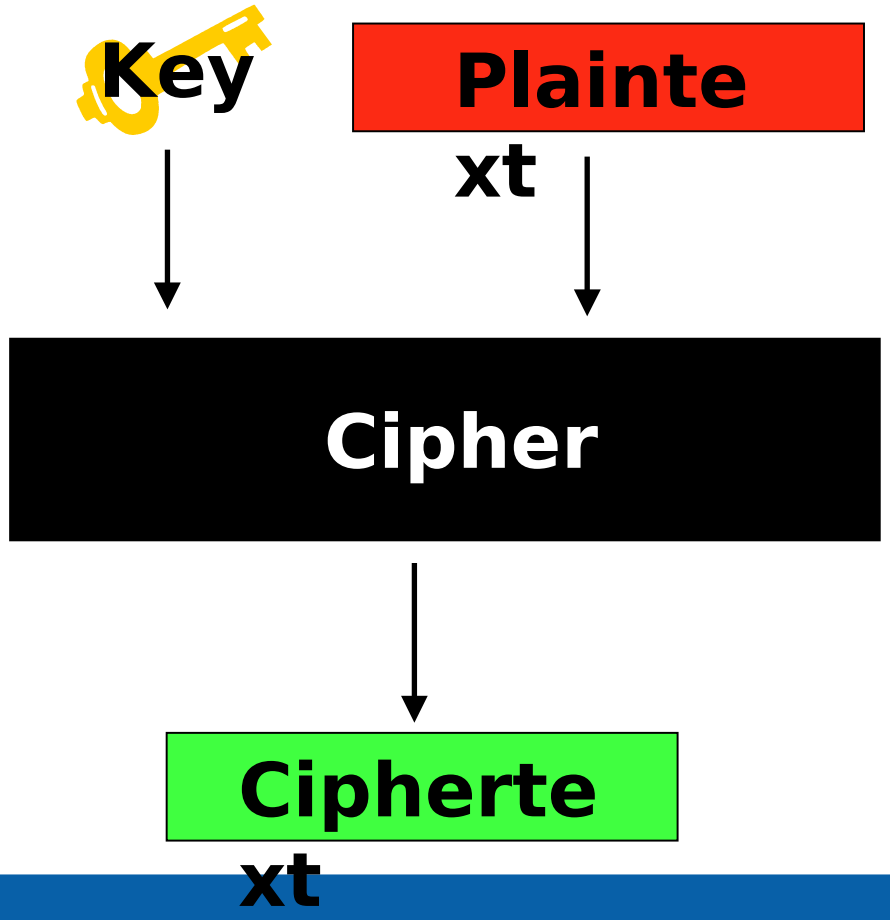
- Wiki : **side channel attack** is any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms.

- Another definition : **side channel attack** is any attack based on information leaked from side channel when system running (All information about : signals, timing, power, sound, …)

- Almost used of side channel attack for **Cryptanalysis**

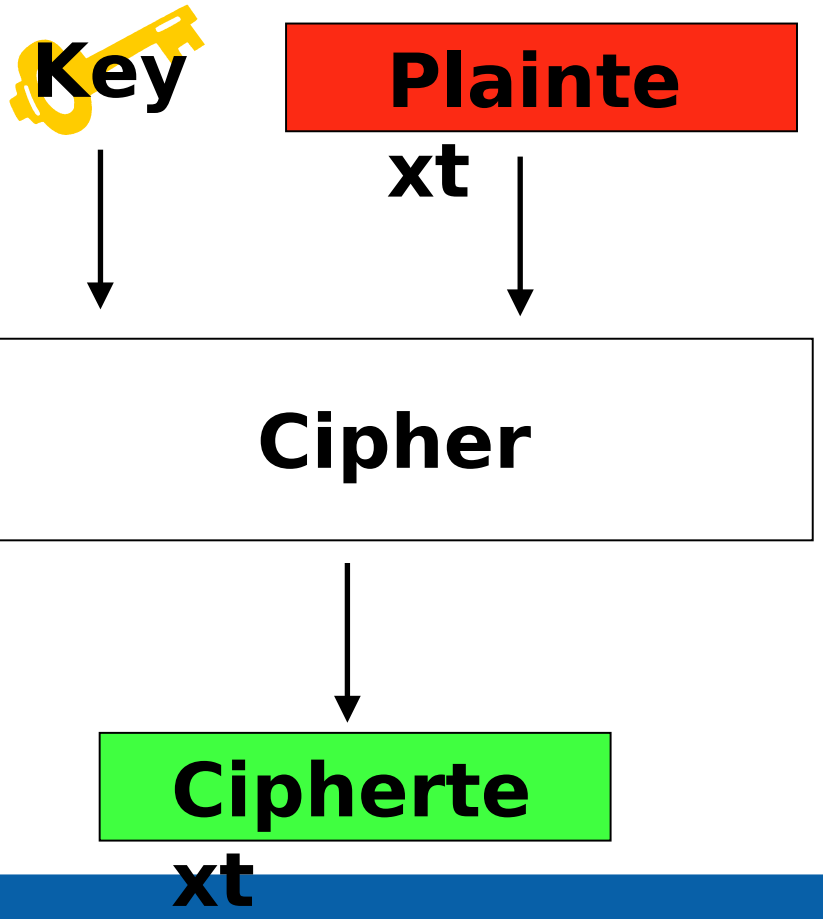
Side channel cryptanalysis

The textbook definition of a cryptosystem:



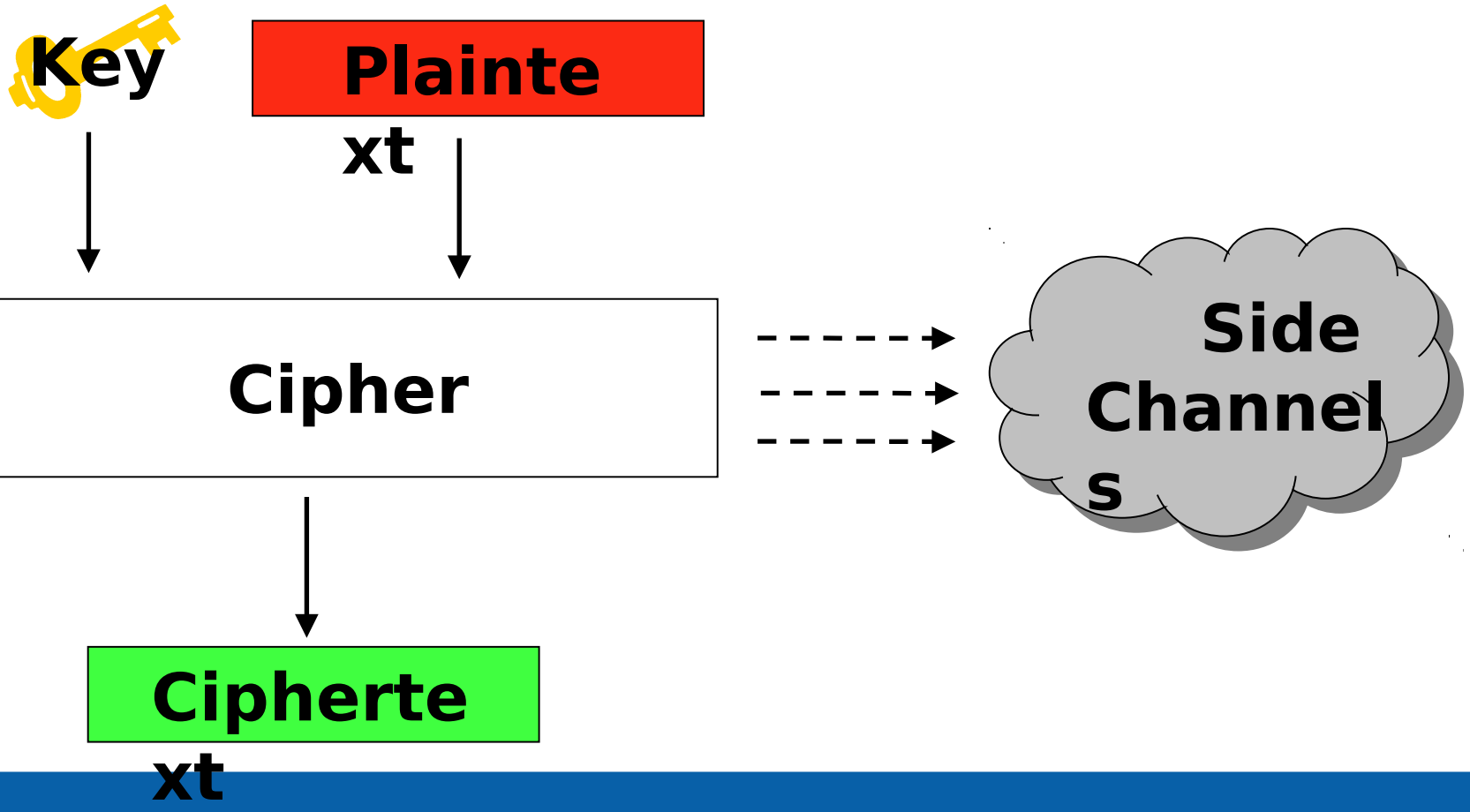
Side channel cryptanalysis

The cryptosystem in real world:



Side channel cryptanalysis

The cryptosystem in real world:

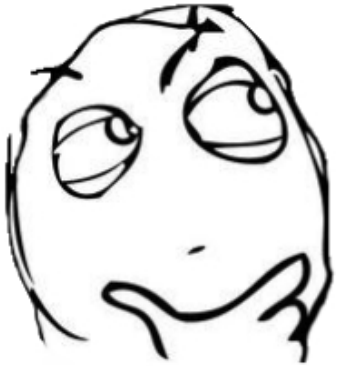


Side channel attacks in the web applications

The big question

Let’s assume an application with none of the top Web vulnerabilities (OWASP Top10, SANS Top25, ...)

What can attackers still do..?



Attack scenarios

- Timing Attacks
- Information leaking
- Cache Attacks

Timing Attacks

- **Using running time of system/program as the side channel to gain the information**

- ***Timing attacks are based on measuring the time it takes for a unit to perform operations. This information can lead to information about the secret data.***

Plaintext Verification Attack

- Imagine we have an authentication system, it's used function pcmp(*p,*i) to compare.
- Func pcmp(string p,string i)

```
int i = 0
for c in ori_pass :
    if(c != input[i]): return False
    else : i = i + 1
return True
```

Plaintext Verification Attack

- Attack…..

Plaintext Verification Attack

- 1. He attempt many password to identify the length of password.
- 2. Cont, he try each char in the password. Differential time of each password let him guess what password is correct .

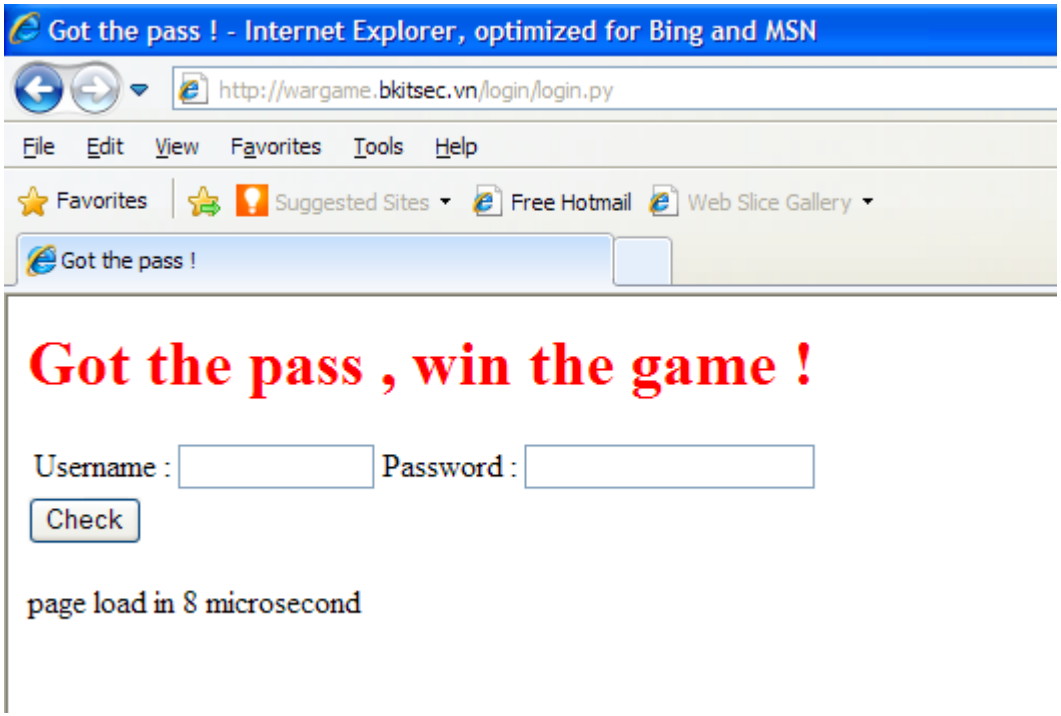
Plaintext Verification Attack

- Best solution for this pcmp
- Func pcmp(string ori_pass,string input)

```
result = True
int i = 0
if len(input) == 0 : return False
if (len(input) > len(ori_pass)) or (len(input) <
  len(ori_pass)):
            input = ori_pass
            result = False
 for c in ori_pass :
            result = result & (input[i] == c)
             i = i + 1
return result
```

Try it!

- http://wargame.bkitsec.vn/login/login.py



Information leaking

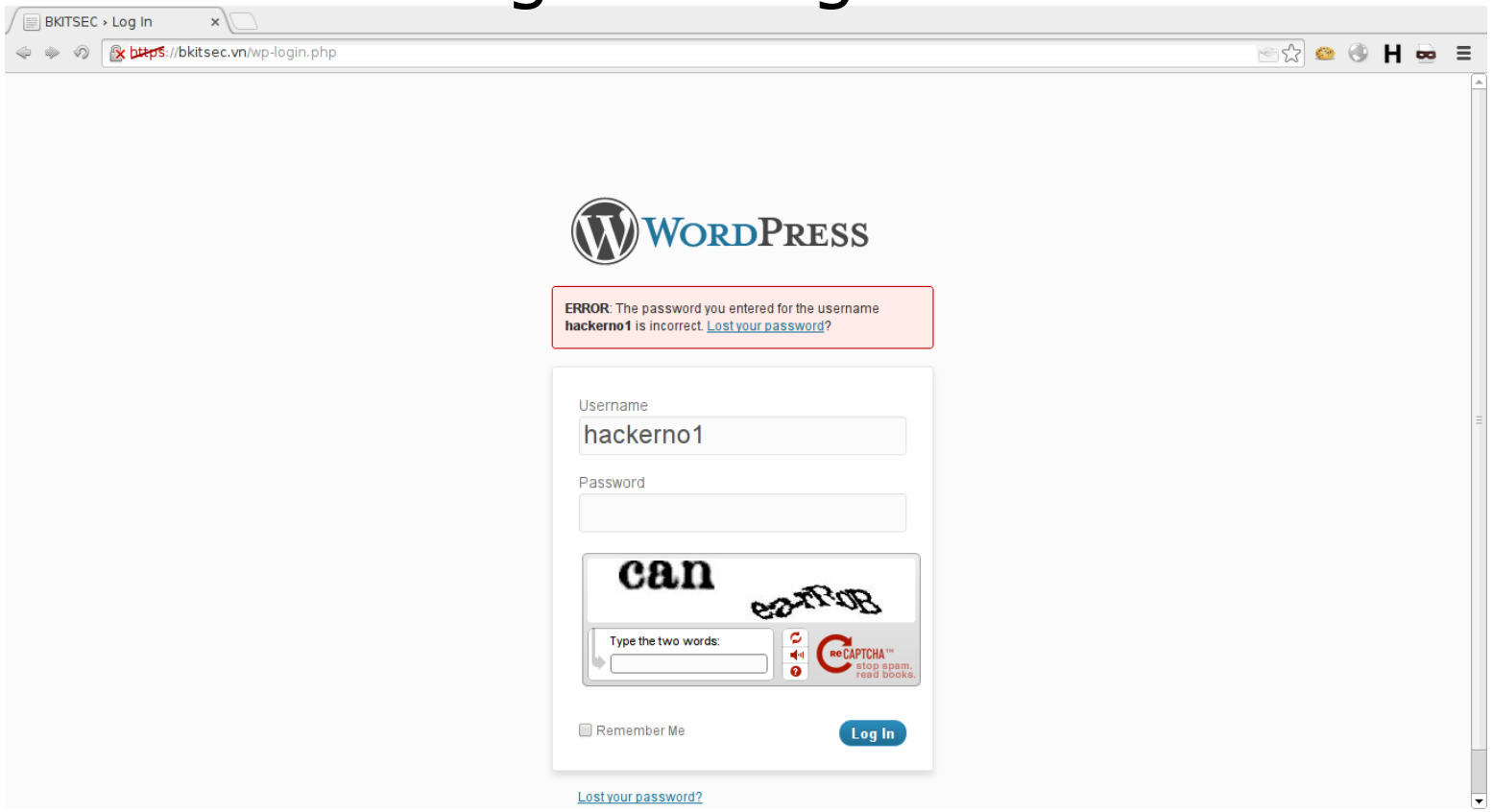
- The side channel in this case is a signal of the program
- The running progress leaked some useful information, hacker can use it to attack the system .

Storage Side Channels

Example for obvious storage side channel:
Error messages of login forms

Storage Side Channels

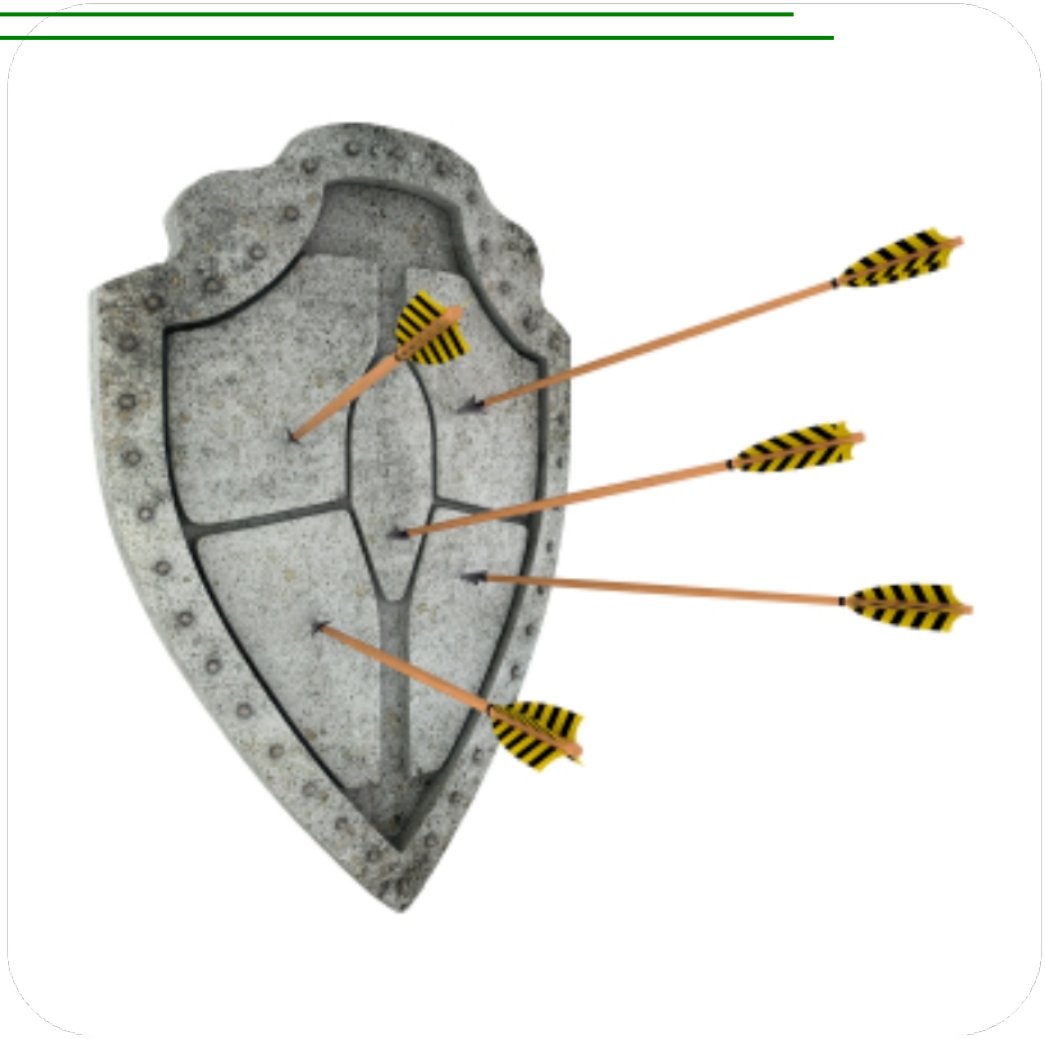
Example for obvious storage side channel:
Error messages of login forms



Storage Side Channels

- Example for obvious storage side channel: Error messages of login forms
  - “Invalid user name” → user name does not exist
  - “Invalid password” → user name exists

Countermeasures



Countermeasures

- Ideal approach:
  - Mathematical model taking into account all side channel characteristics
  - Design crypto systems basing on this model
- 100% Impossible - Difficulties:
  - Large number of parameters
  - Different type of traces

Countermeasures

- Software Solutions:
  - Constant execution paths
  - Avoid conditional branches
  - Hashing values before using them
- Creative coding
- Performance penalties

Conclusions

- Side channels can appear in various ways.

  Detection is difficult

- Side Channel Attacks highlight the need for **co-working** of software, hardware, algorithm & protocol designers

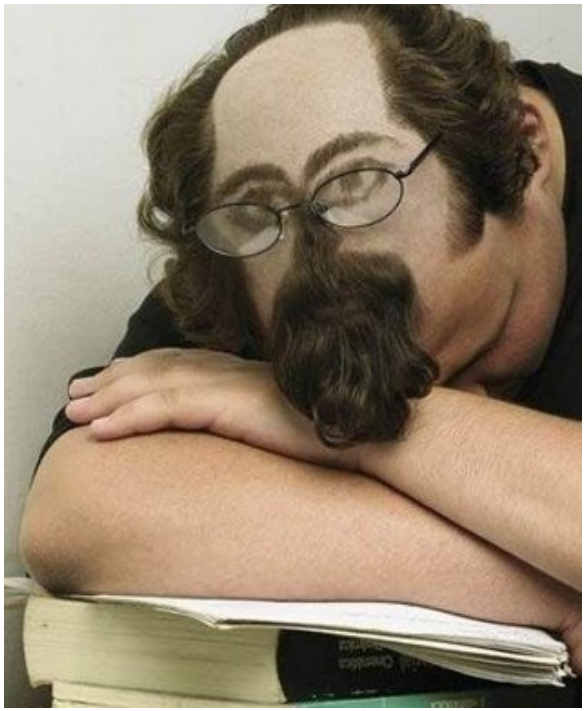
- Side channel attacks are passive

  Attacks are feasible for a skilled attacker

- Prevention strategies may have a negative impact on system performance.

  Prevention is difficult

Hey, guys ... wake up !!!
It's time to question



Q & A