UNIVERSITY OF TWENTE.

Side channels

Topic of Software Systems (TCS module 2)

Lecturer: Maarten Everts

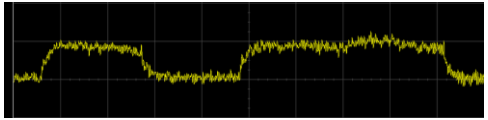
SIDE-CHANNEL ATTACKS

Whenever your program deals with secret information, it may leak information about them:

Timings

Power usage

Cache misses



One of the reasons to use proper libraries!

SIDE-CHANNEL ATTACK EXAMPLE

Suppose:

- A simple networked service
- Password-protected
- Password is sent in plaintext — For simplicity, typically a bad idea
- Password: exactly 8 characters (a-z, A-Z, 0-9)

```
public boolean checkPassword(String input)
```

Number of different characters: 26+26+10 = 62

Number of possible passwords: 62^8 = 218340105584896 (≈ $2*10^{14}$)

SIDE-CHANNEL ATTACK EXAMPLE

```java
private String secretPassword = "Secret12";
public boolean checkPassword(String input) {
    if (input.length() != secretPassword.length()) {
        return false;
    }
    for (int i = 0; i < input.length(); i++) {
        if (input.charAt(i) != secretPassword.charAt(i)) {
            return false;
        }
    }
    return true;
}
```

Suppose: 1 iteration ~10μs

Given timing information:

input = “AAAAAAAA” vs. input = “SecAAAAA”?

input = “AAAAAAAA” vs. input = “BAAAAAAA”?

input = “AAAAAAAA” vs. input = “SAAAAAAA”?

input = “SAAAAAAA” vs. input = “SeAAAAAA”?

input = “SeAAAAAA” vs. input = “SecAAAAA”?

Algorithm for side-channel attack!

8*62 = 496 attempts

vs.

62^8 = 218340105584896 attempts

Meltdown and Spectre

Vulnerabilities in modern computers leak passwords and sensitive data.

Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware vulnerabilities allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents.

Meltdown and Spectre work on personal computers, mobile devices, and in the cloud. Depending on the cloud provider's infrastructure, it might be possible to steal data from other customers.

Meltdown

Spectre

Security

Meltdown, Spectre bug patch slowdown gets real – and what you can do about it

Chip flaw fixes not so insignificant after all

By Thomas Claburn in San Francisco 9 Jan 2018 at 00:45 129 SHARE ▼

Analysis Having shot itself in the foot by prioritizing processor speed over security, the chip industry's fix involves doing the same to customers.

The patches being put in place to address the Meltdown and Spectre

Most read


Ticketmaster tells customer it's not at fault for site's Magecart malware pwnage


Windows 10 can carry on slurping even when you're sure you yelled STOP!


Having swallowed its pride and started again with 10nm chips, Intel teases features in these 2019-ish processors


Here's 2018 in a nutshell for you... Russian super robot turns out to be man in robot suit


It is with a heavy heart that we must inform you hackers are targeting 'nuclear, defense, energy, financial' biz

USING CRYPTOGRAPHY, WORDS OF WARNING

DO NOT invent your own crypto!

- It will be broken!
- Only do it for fun (and learning)!

DO NOT even implement cryptographic primitives yourself!

- So many details to get right
- “It is typically not the math that is broken, it’s the implementation”

Rules of thumb

- Data at rest: use pgp/gpg
- Data in motion: use (SSL/)TLS

But be careful!

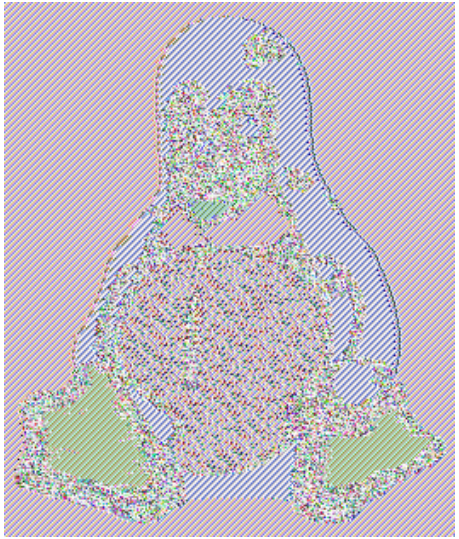
USE *high-level* cryptographic libraries!

Preferably open source!

- NaCl (“salt”): http://nacl.cr.yp.to/
- Keyczar: http://www.keyczar.org/

WHY?

“We’ll just use encryption, AES appears to be good, yes?”



AES in the ECB mode-of-operation applied to a image

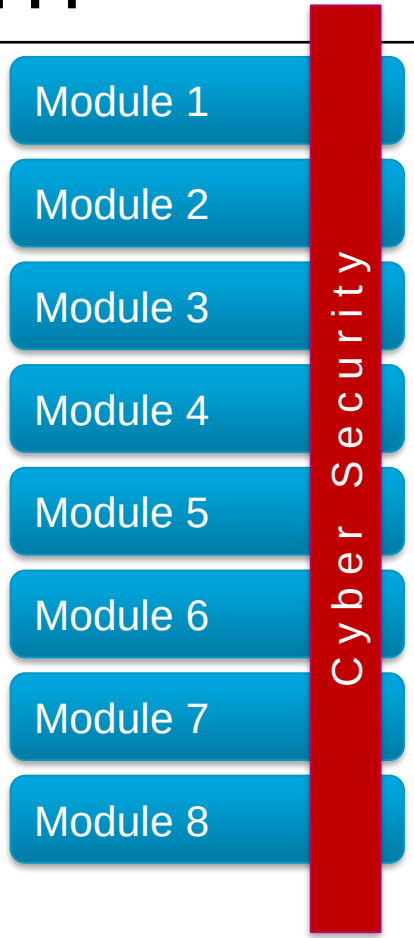
UNIVERSITY OF TWENTE.

Side channels

Topic of Software Systems (TCS module 2)

Lecturer: Maarten Everts

WANT MORE SECURITY?



The 4TU cyber security master specialisation:
https://www.4tu.nl/cybsec/en/

UNIVERSITY OF TWENTE.

MOOC: Coursera's course on Cryptography by Dan Boneh (Stanford)
https://www.coursera.org/course/crypto

MOOC: Coursera's course on Software Security by Michael Hicks
https://www.coursera.org/course/softwaresec

Twente Hacking Squad:
See http://scs.ewi.utwente.nl/home/TwenteHackingSquad/ for more info.

UNIVERSITY OF TWENTE.