Protect Your Screen From Eavesdropping

Don't Forget Its Power Supply

Emmanuel COTTAIS

ANSSI - National Cyber Security Agency of France

About the author

- ANSSI: National Cyber Security Agency of France
- Wireless Security Lab
  - 11 members (4 PhDs, 1 PhD student)
  - Wireless Communications Security (mobile communication, Wi-Fi, Bluetooth, RFID, etc.)
  - Embedded Systems
  - Physical layer
  - Signal Processing
  - Electromagnetic Security (TEMPEST, IEMI)
- Emmanuel COTTAIS
  - PhD in electronics
  - Electromagnetic security Expert
  - TEMPEST team leader

TEMPEST: what will we talk about?

Google gives many different results:

WWII fighter

Future RAF fighter

TEMPEST: what will we talk about?

Google gives many different results:

Sailboat

Capelli®boats range

TEMPEST: what will we talk about?

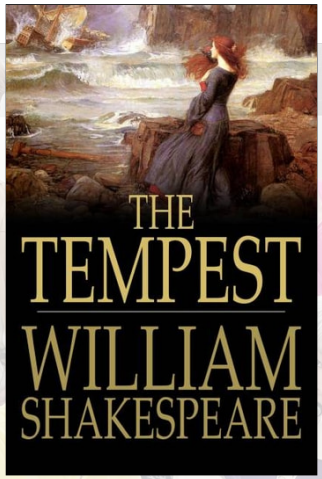
Google gives many different results:

K-pop group

Metal group

TEMPEST: what will we talk about?

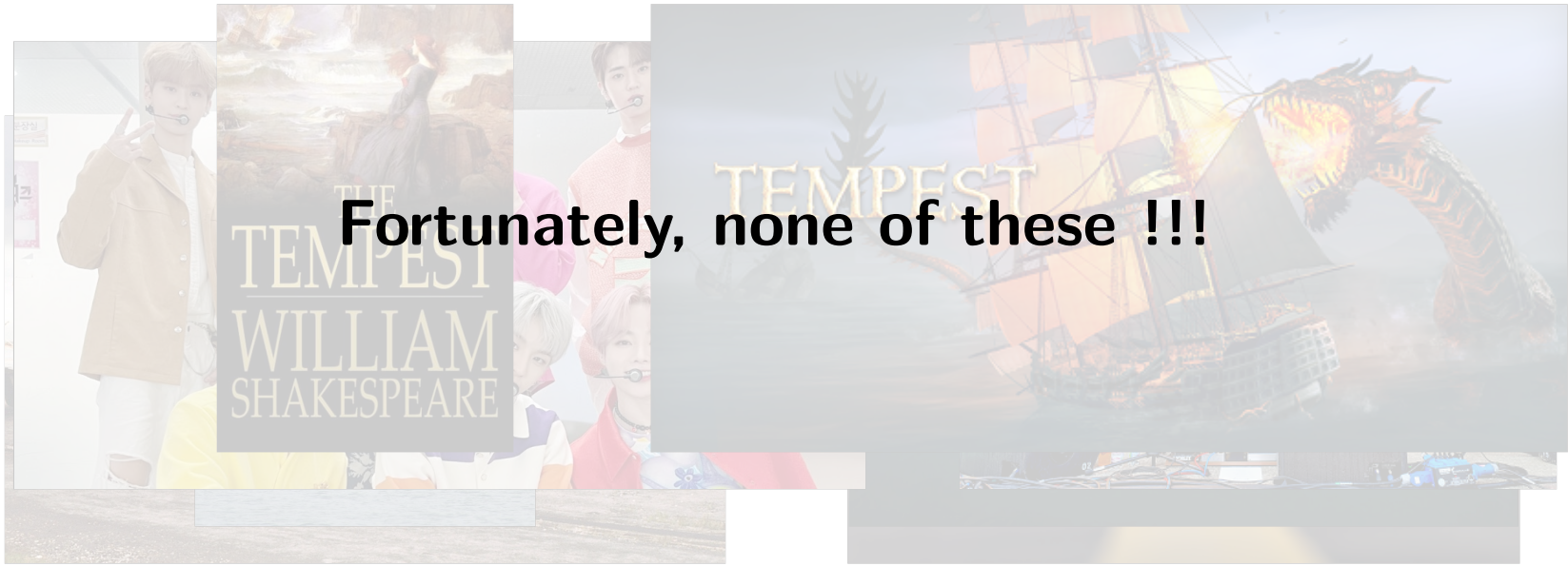
Google gives many different results:



Shakespeare drama

Video game

TEMPEST: what will we talk about?



Fortunately, none of these !!!

TEMPEST: what will we talk about?

Electromagnetic emanations

- Origin
- Impacts on security
- How to protect sensitive data?

Agenda

1. The TEMPEST threat
2. Protection strategy against electromagnetic emanations
3. Live demo

Agenda

1. The TEMPEST threat
   - Electromagnetic compatibility (EMC)
   - Link between EMC, IT security and TEMPEST
   - Origin of electromagnetic emanations
   - Potential leakage paths
   - Most risky case
2. Protection strategy against electromagnetic emanations
   - Global principle
   - Best protection: shielded enclosure
   - Protection from equipment
   - Protection from building
   - Balanced protection
3. Live demo

Sommaire

Electromagnetic compatibility (EMC)

- EMC gives a set of rules to assure that electronic equipment can work close to each other

Electromagnetic compatibility (EMC)

- EMC is based on 2 fundamental principles
  - Emissivity of parasitic signals
    - Can't be canceled, always present, more or less powerful
    - Should not be too much powerful to cause perturbations on other equipment around

Electromagnetic compatibility (EMC)

- EMC is based on 2 fundamental principles
  - Emissivity of parasitic signals
    - Can't be canceled, always present, more or less powerful
    - Should not be too much powerful to cause perturbations on other equipment around
  - What consequences of EMC emissivity?

source: anfr

LES ENQUÊTES DE L'ANFR - LE SON QUI COUPAIT LA 4G

08/04/2021

Le service régional de l'ANFR basé à Aix-en-Provence est récemment intervenu pour résoudre un brouillage quelque peu inattendu...

Sur la commune de Sernhac dans le Gard et dans une zone de 10 km alentour, les services 4G dans la bande 800 MHz ne répondaient plus ! La seule antenne-relais de la commune ainsi qu'une autre située à 6 km étaient affectées par un mystérieux signal perturbateur.

Un agent du contrôle du spectre, doté d'une « artillerie » de pointe, s'est donc rendu sur place pour mener une véritable investigation technique : les relevés spectraux permirent dans un premier temps d'obtenir la signature du signal perturbateur, c'est-à-dire l'émission électromagnétique caractéristique d'un objet. Il fallait maintenant trouver d'où provenait ce signal... Le récepteur du véhicule laboratoire et une antenne Yagi directive orientèrent les recherches, qui menèrent l'agent chez un particulier, dans un village à 3 km de l'une des deux antennes-relais brouillées. Avec l'accord du propriétaire, les investigations se poursuivirent à son domicile pour finalement aboutir à l'objet ... qui n'était autre qu'un casque audio sans fil ! Cet équipement, largement utilisé en ces temps de télétravail renforcé, apparaissait au premier abord inoffensif. Mais il émettait en fait en dehors de sa bande de fréquences allouée et empiétait sur celle de la 4G qui émettait en bande 800 MHz. Le casque brouillait même sur plusieurs kilomètres à la ronde ! Bien que disposant d'un marquage CE, il s'était mis à dériver avec le temps. Impossible pour le propriétaire de s'en rendre compte : le casque fonctionnait parfaitement bien ! Après l'avoir débranché, la perturbation de la 4G identifiée sur 10 km disparut instantanément.

Electromagnetic compatibility (EMC)

- EMC is based on 2 fundamental principles
  - Susceptibility of an equipment
    - Ability to work inside an electromagnetic environment
    - Should not be too much weak to take into account other equipment working around

Electromagnetic compatibility (EMC)

- EMC is based on 2 fundamental principles
  - Susceptibility of an equipment
    - Ability to work inside an electromagnetic environment
    - Should not be too much weak to take into account other equipment working around
  - What consequences of EMC susceptibility?

Fishbowl operation

High-altitude nuclear tests – 1962

400km above the Pacific Ocean

Impacts 1445 km away, in Hawaii

source: wikipedia.org

Electromagnetic compatibility (EMC)

- EMC is based on 2 fundamental principles
  - Emissivity of parasitic signals
  - Susceptibility of an equipment
- Since 2014 (Directive EU/2014/30) UE includes EMC aspects for all electronic devices to be sent in UE market

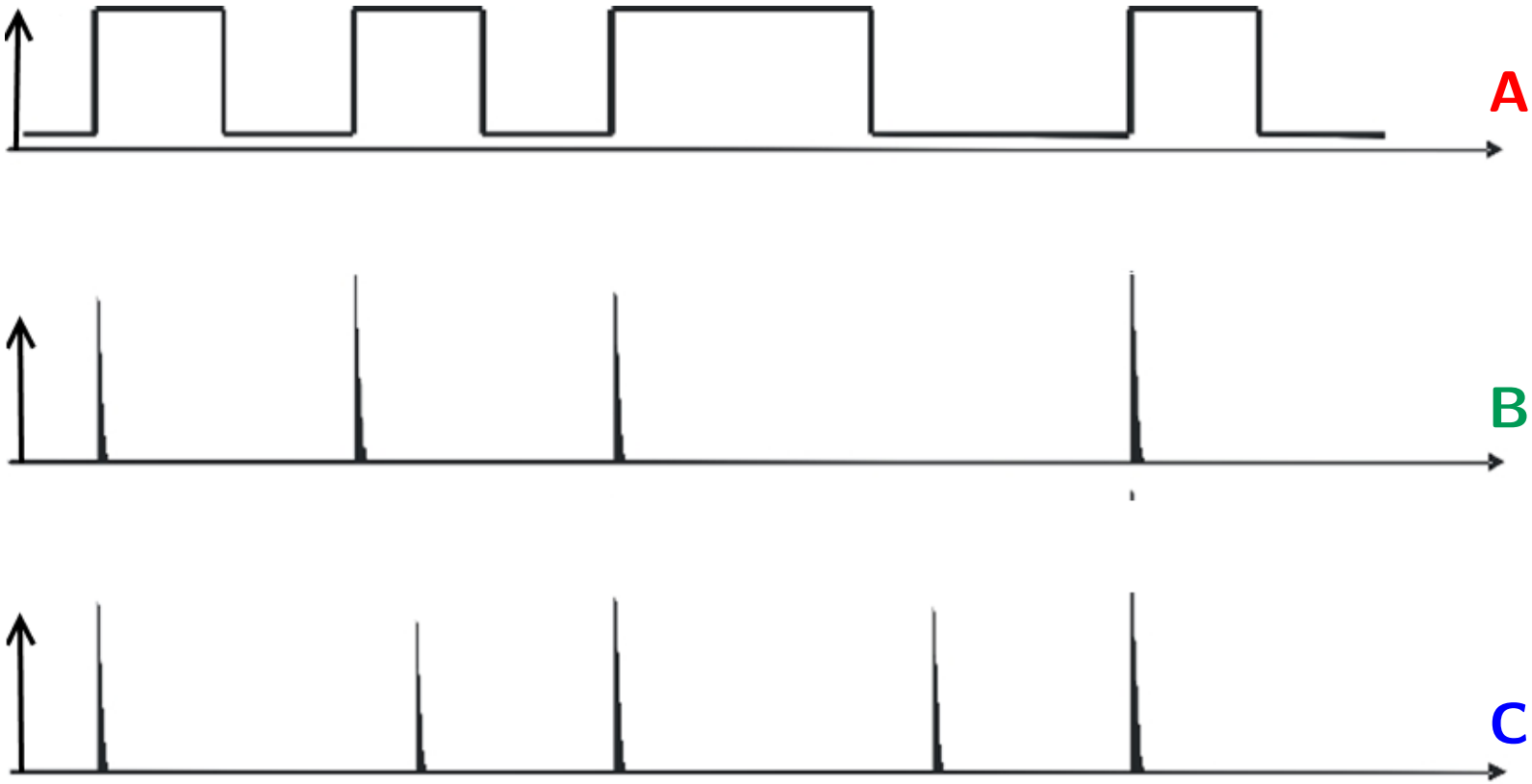
Sommaire

Risk linked to emissivity

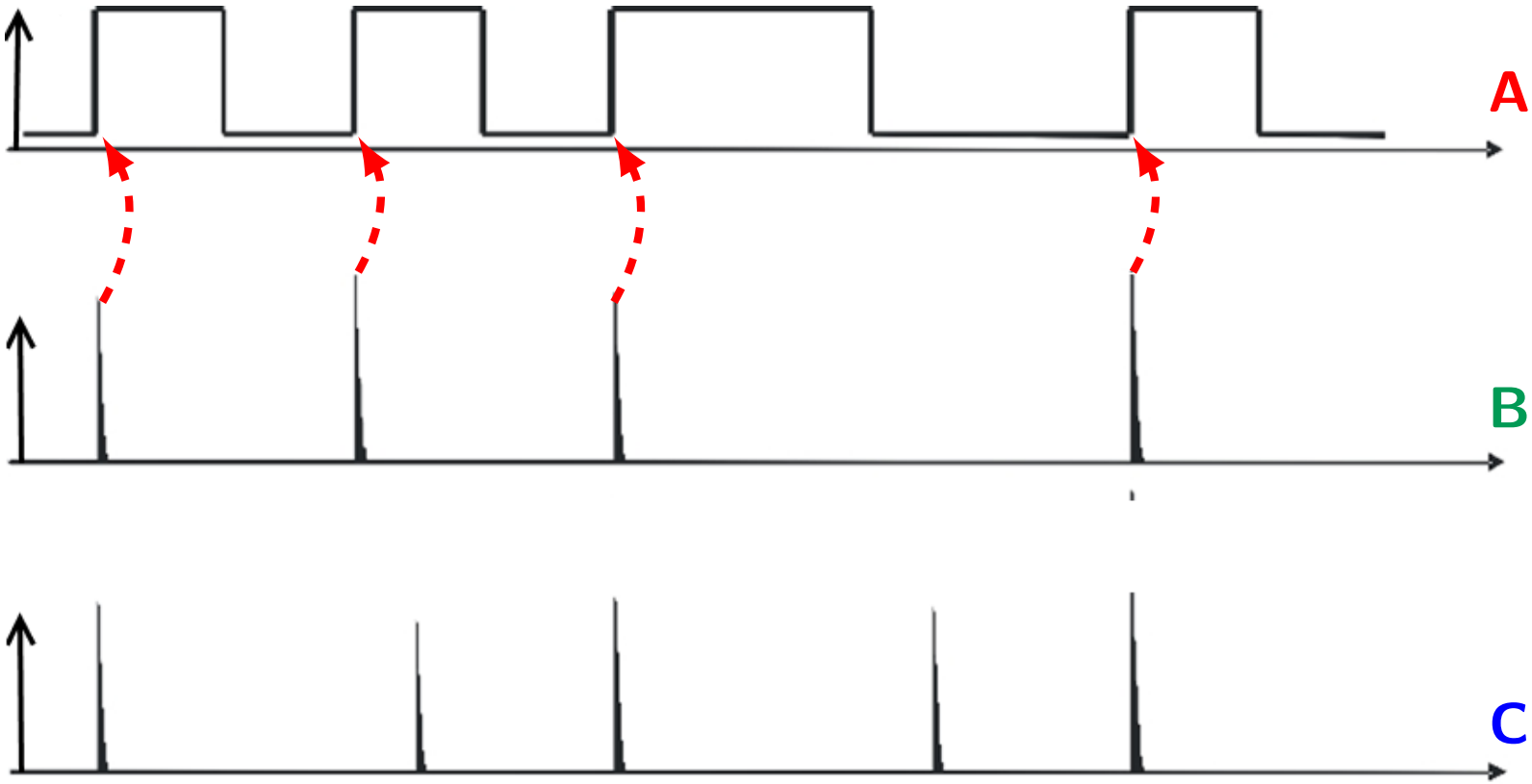
Risk linked to emissivity

Confidentiality may be broken if compromising emanations

Risk linked to emissivity

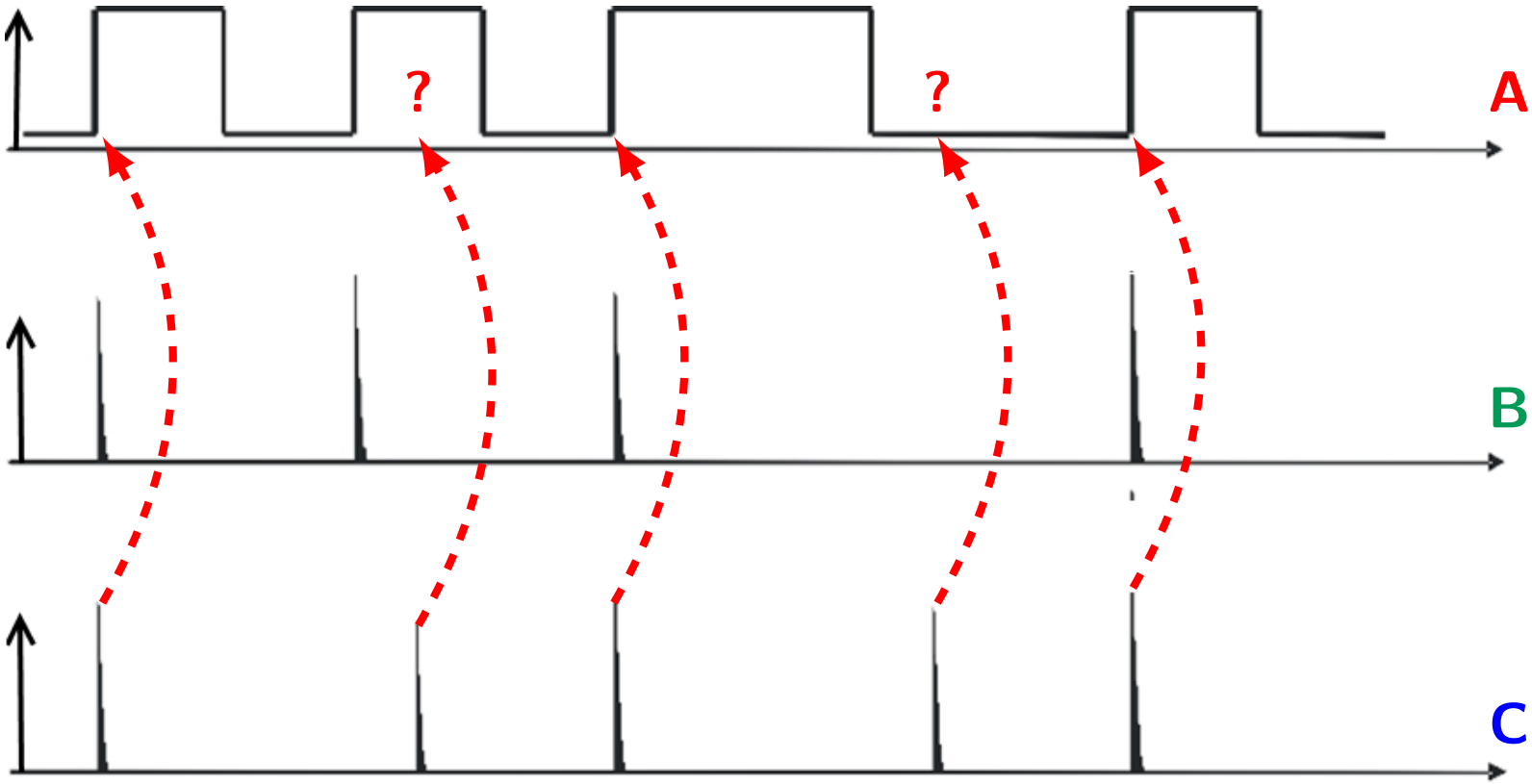


Risk linked to emissivity



A can be regenerated from B $\Longrightarrow$ B is compromising

Risk linked to emissivity



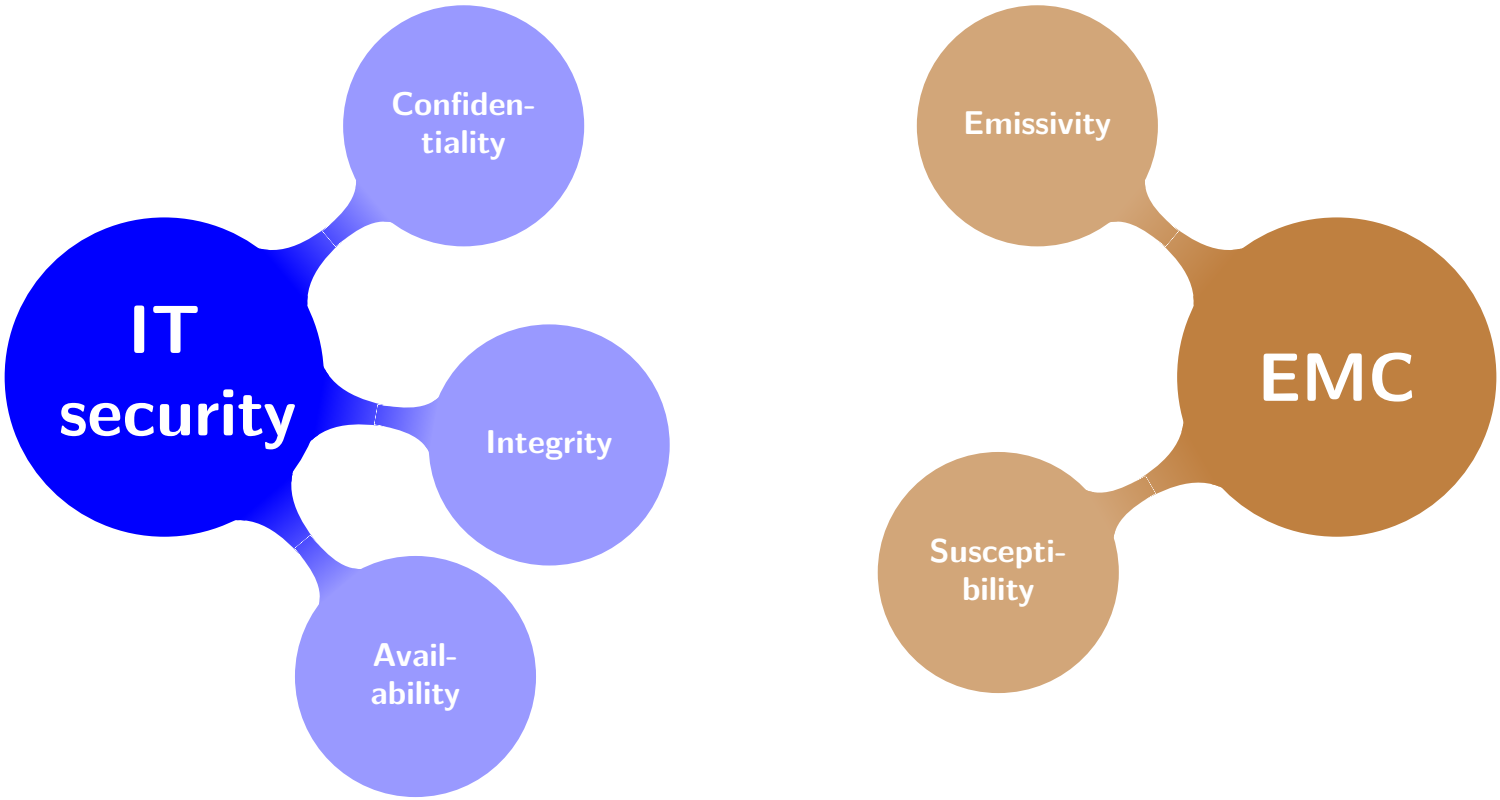
A can't be regenerated from C $\Longrightarrow$ C is not compromising

Risk linked to susceptibility

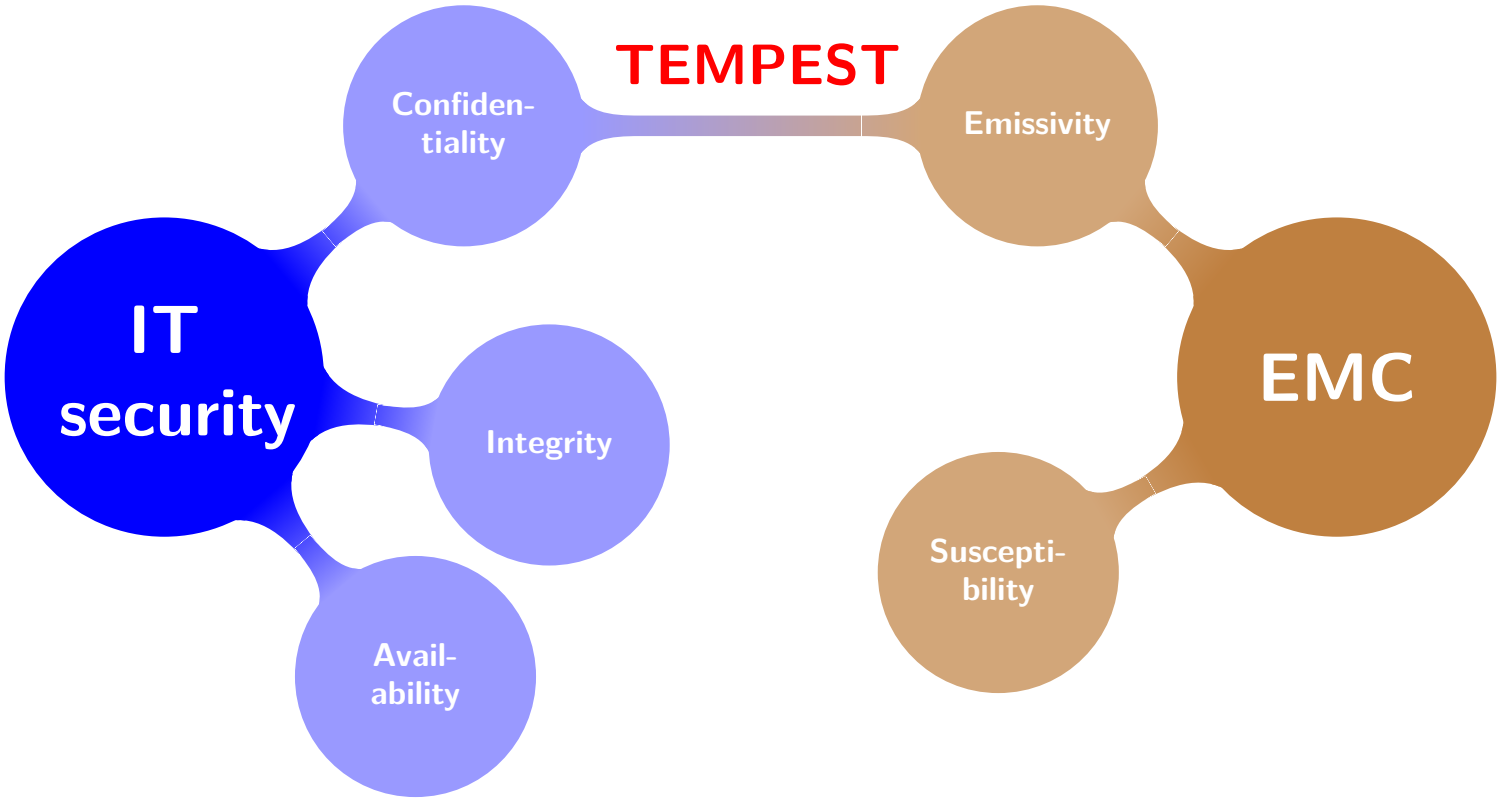
Risk linked to susceptibility

Integrity and/or availability may be broken

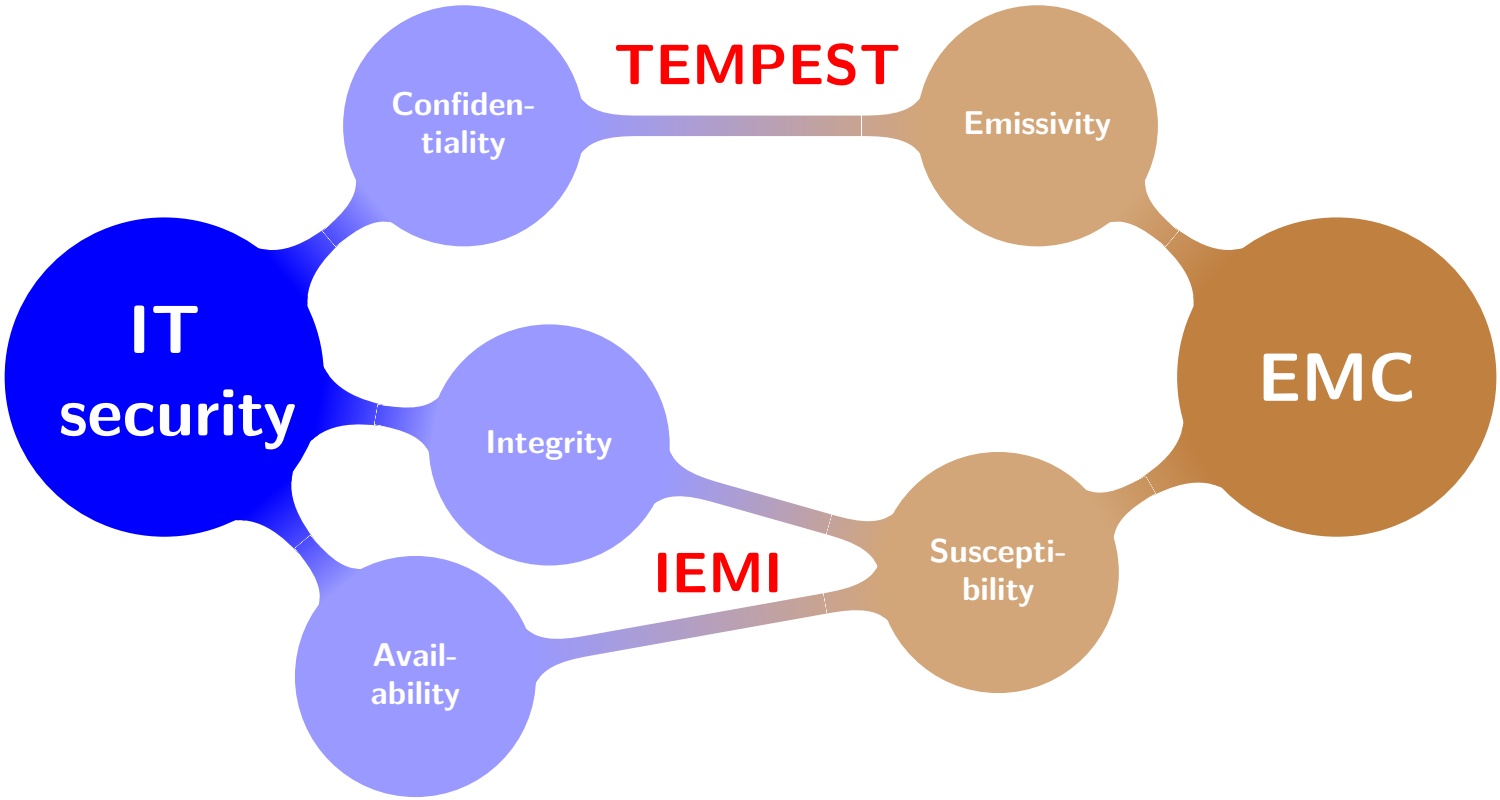
Link between EMC and TEMPEST



Link between EMC and TEMPEST



Link between EMC and TEMPEST

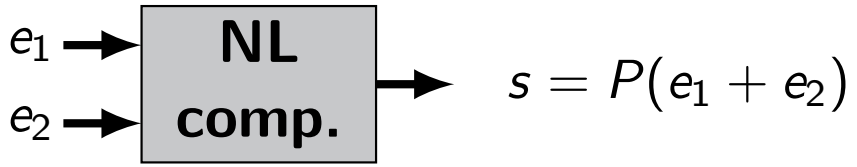


Sommaire

Electromagnetic emanations: origin

Electromagnetic emanations: origin

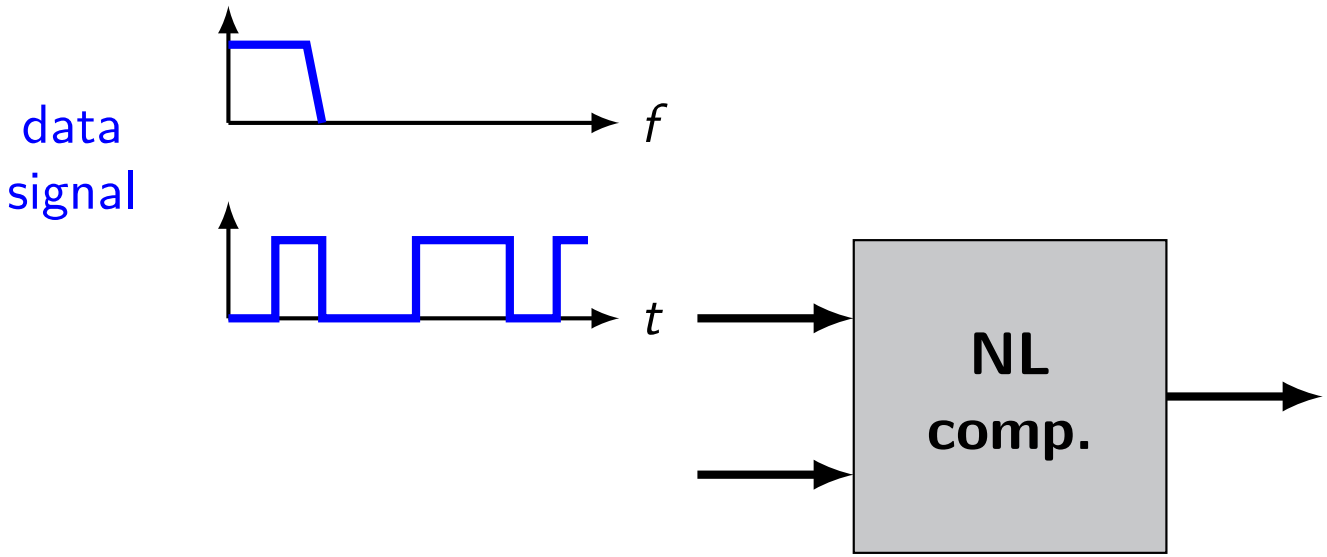
Any electronic board contains nonlinear components which generate undesired amplitude modulations



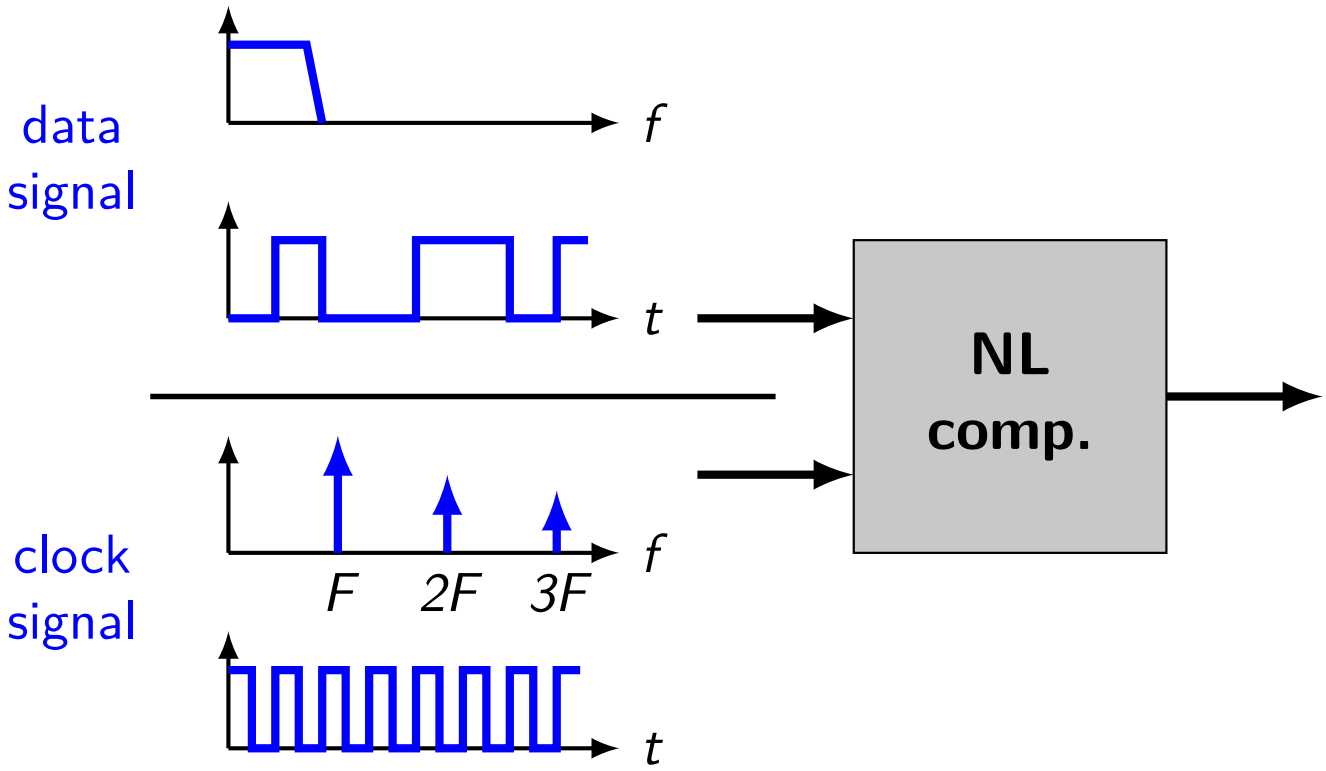
$$P(x) = a_0 + a_1.x + a_2.x^2 + a_3.x^3 + \dots$$

Electromagnetic emanations: origin

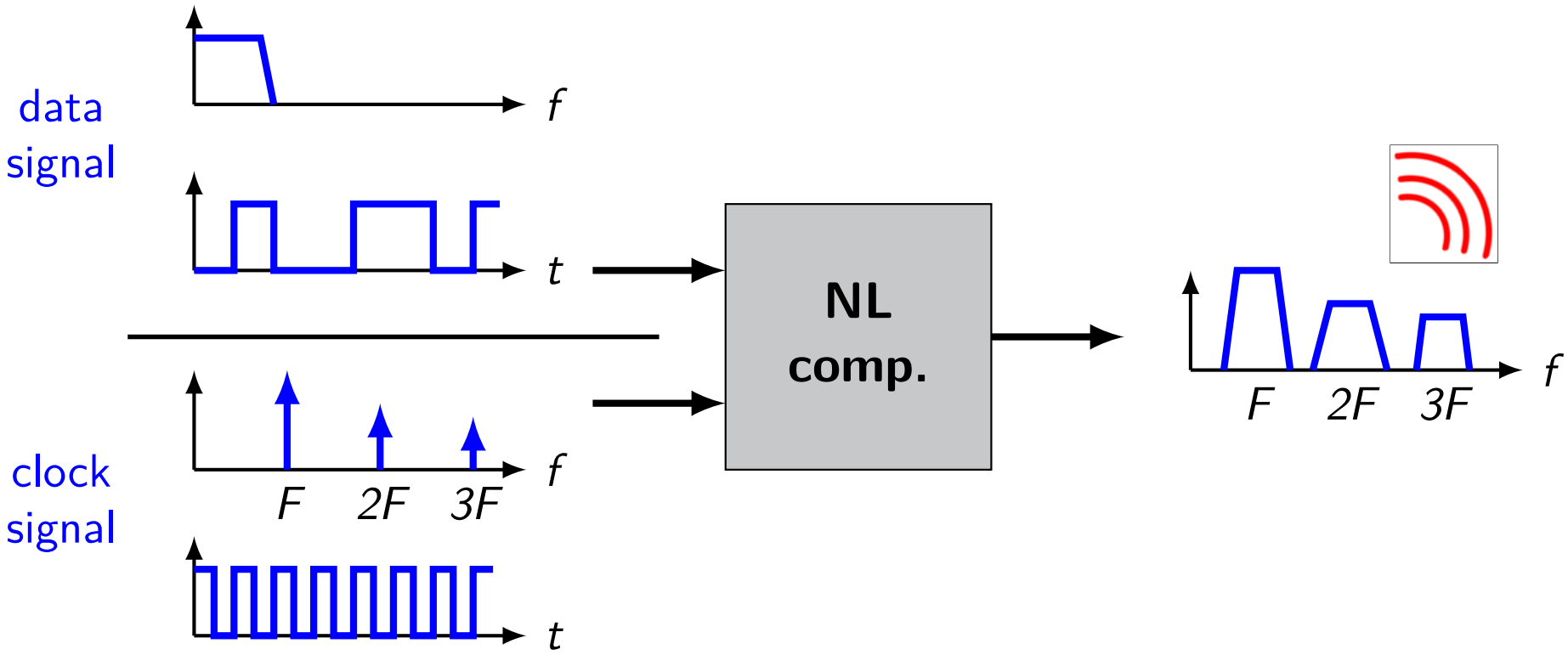
Electromagnetic emanations: origin



Electromagnetic emanations: origin

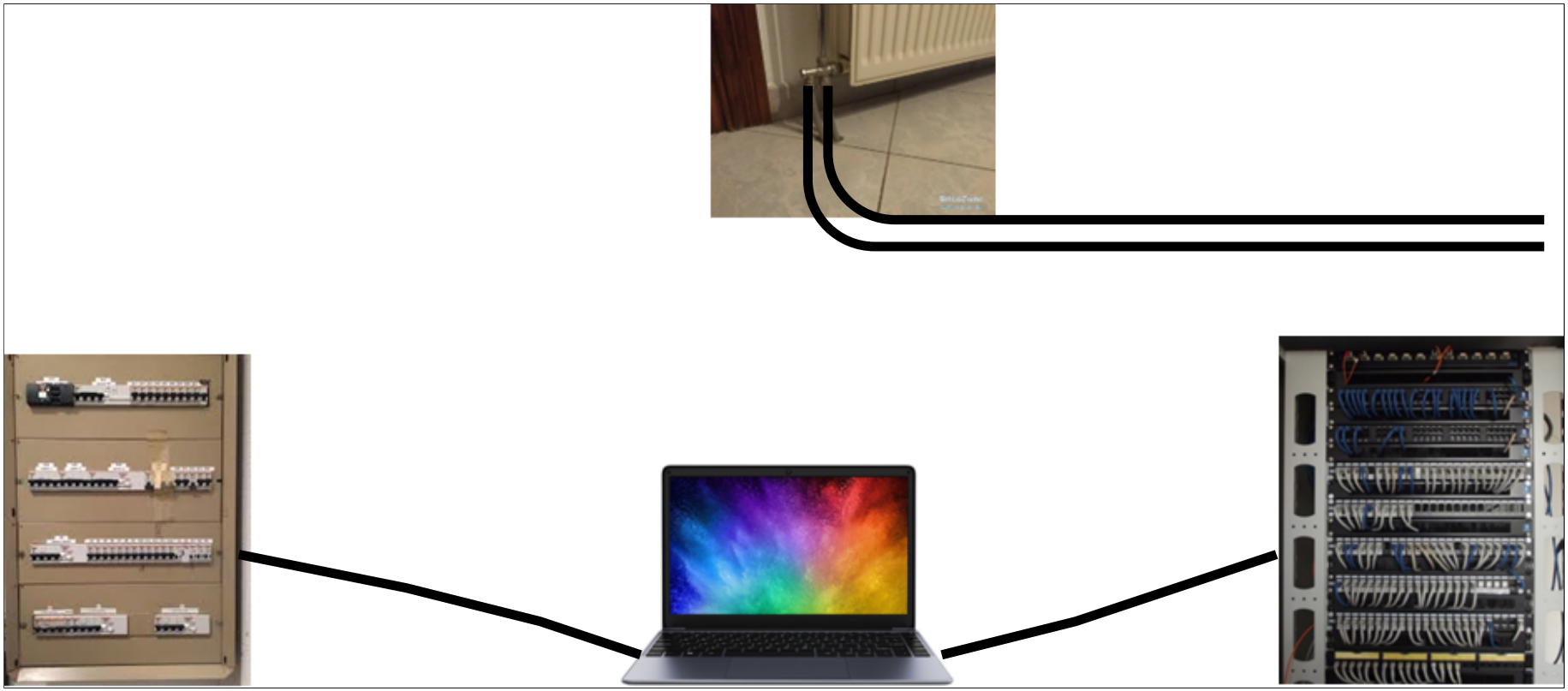


Electromagnetic emanations: origin



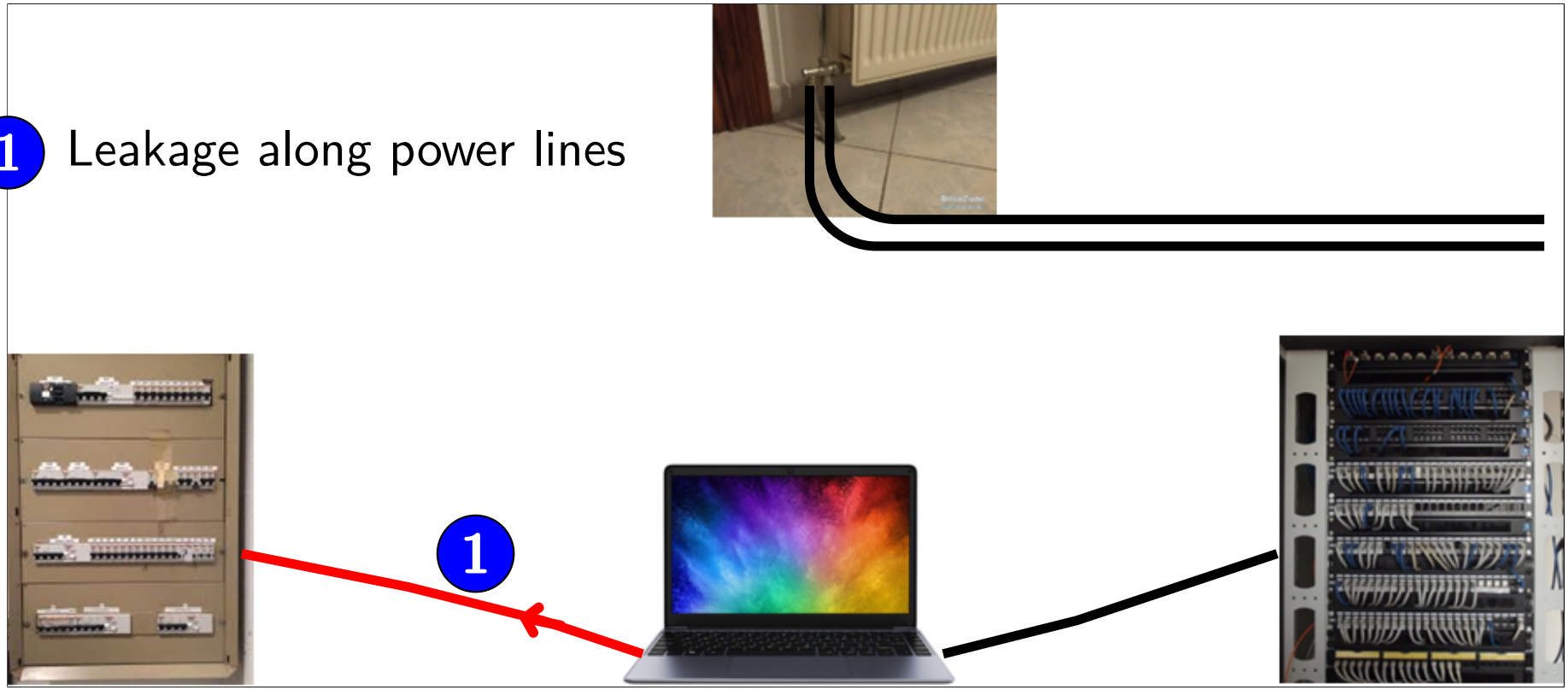
Sommaire

Electromagnetic emanations: potential leakage paths



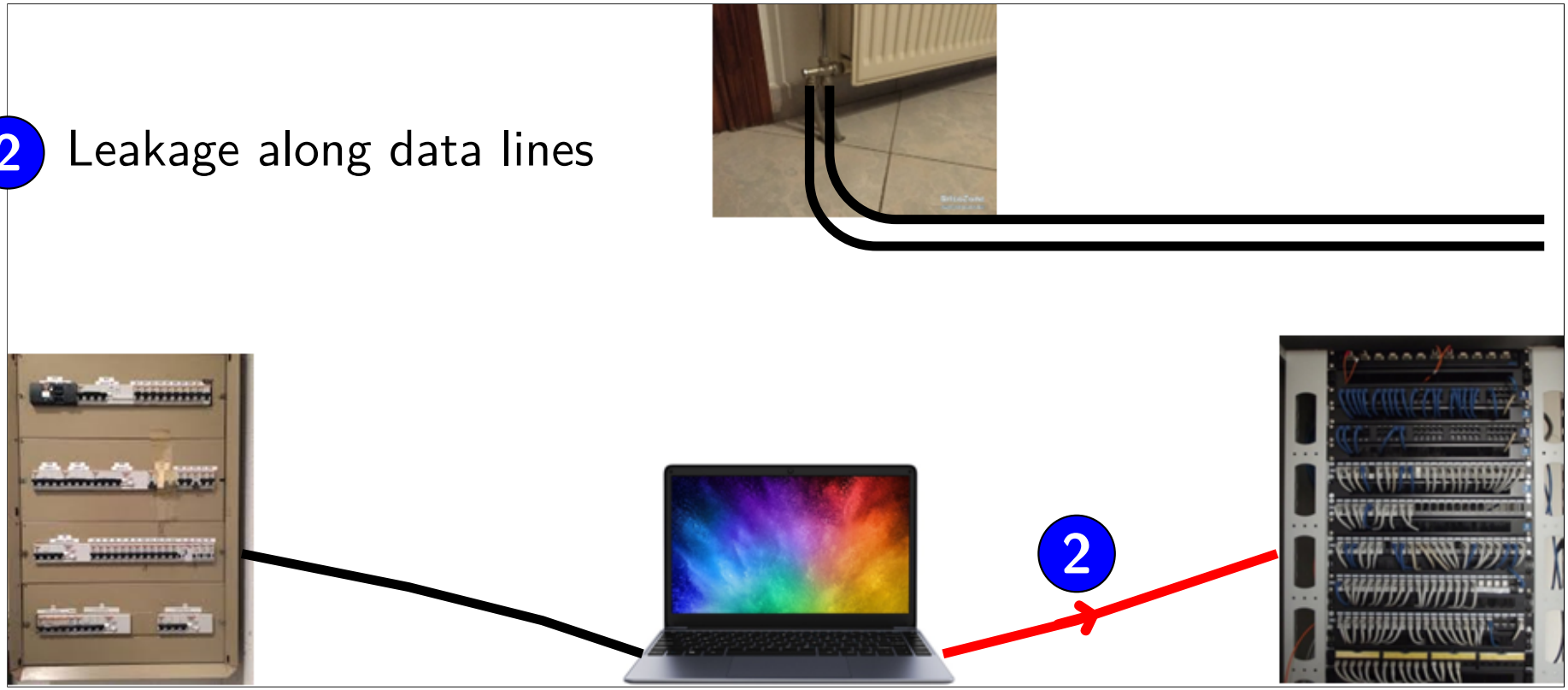
Electromagnetic emanations: potential leakage paths

1 Leakage along power lines

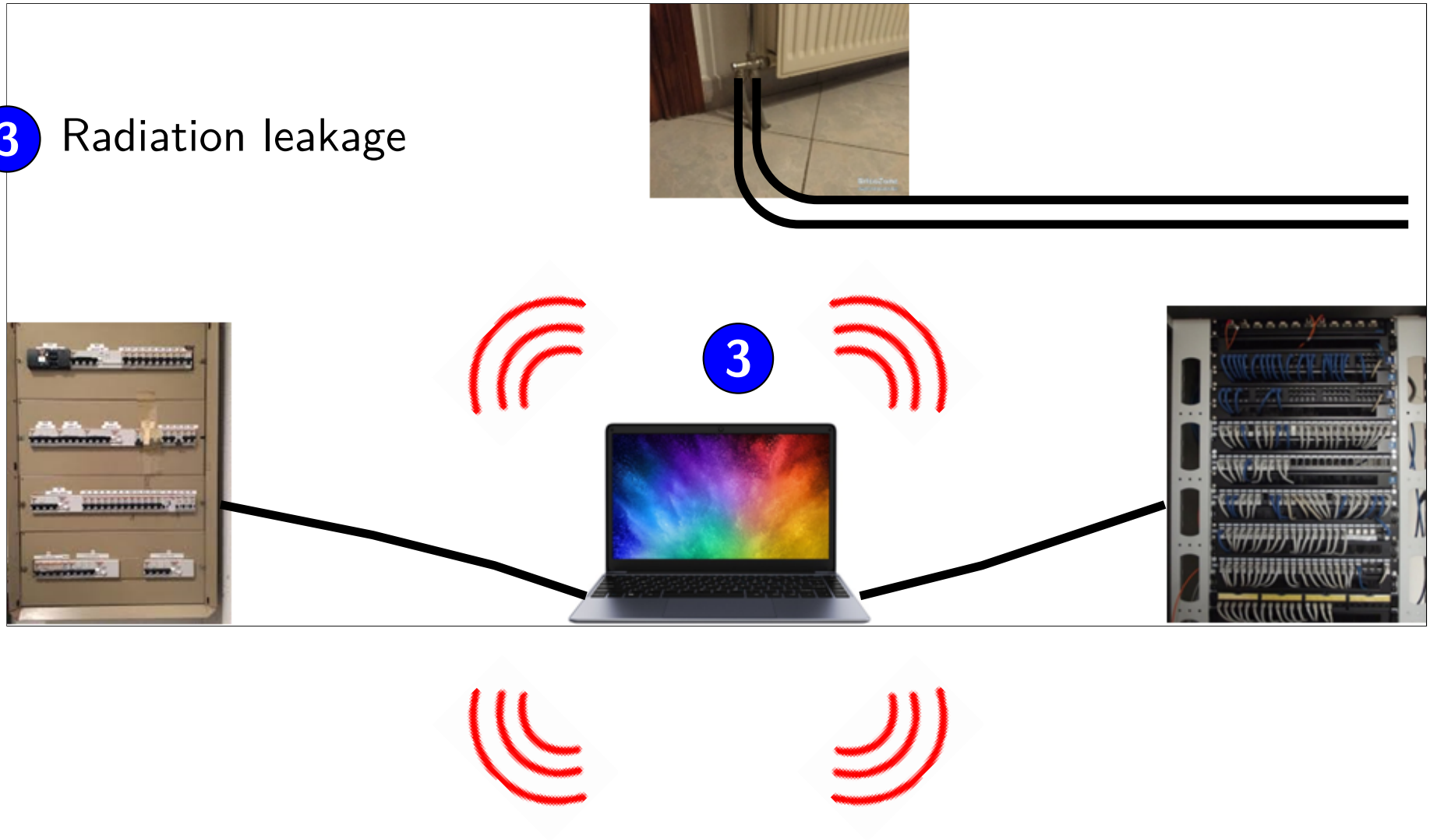


Electromagnetic emanations: potential leakage paths

2 Leakage along data lines



Electromagnetic emanations: potential leakage paths



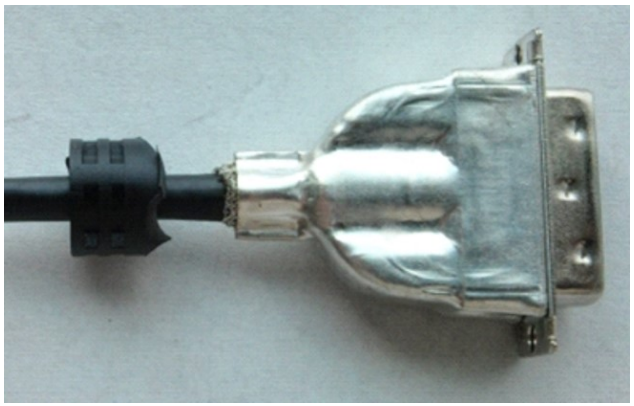
Electromagnetic emanations: potential leakage paths

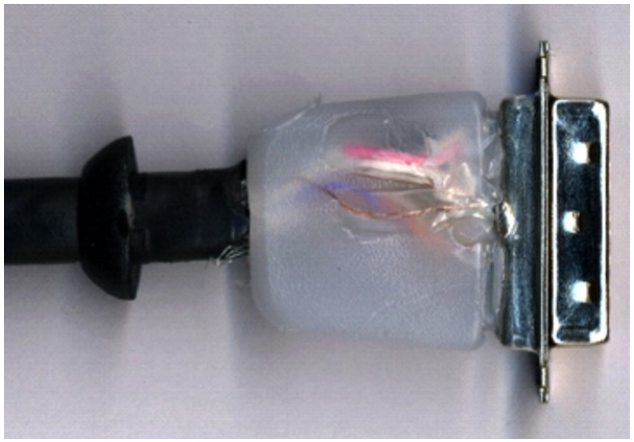
4 Leakage along fortuitous metallic conductors

4

Sommaire

Most risky case: video signal



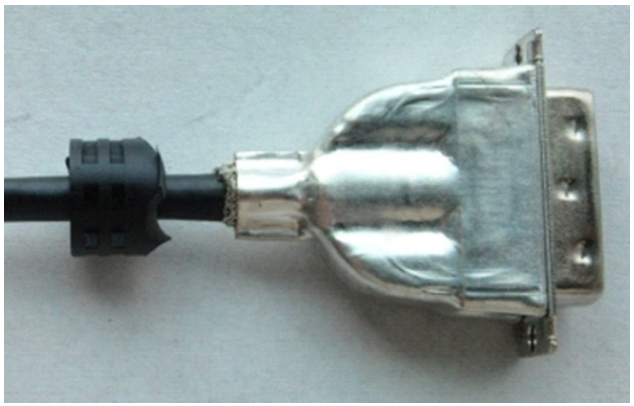


Video signal is repetitive (60 frames/sec)

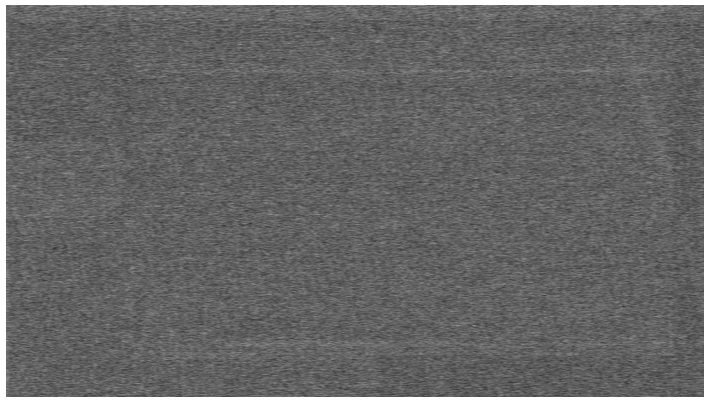
Averaging is easy to improve quality

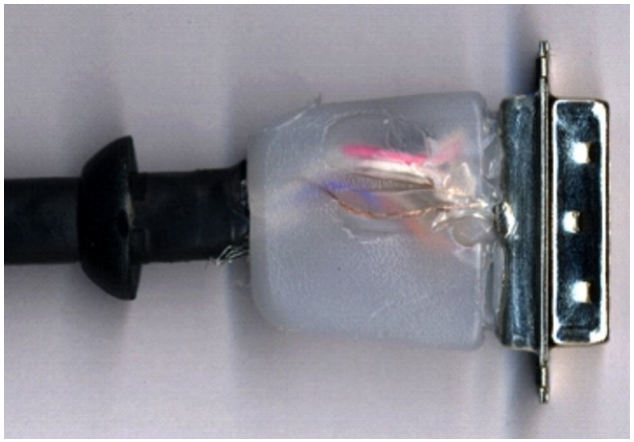
Leakage amplified by badly shielded connectors

Most risky case: video signal



shielded connector



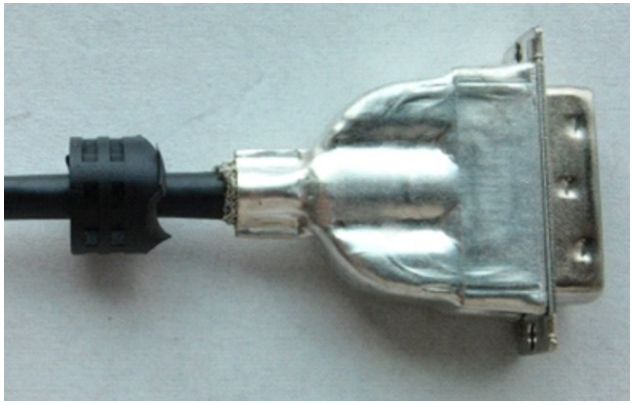


Video signal is repetitive (60 frames/sec)

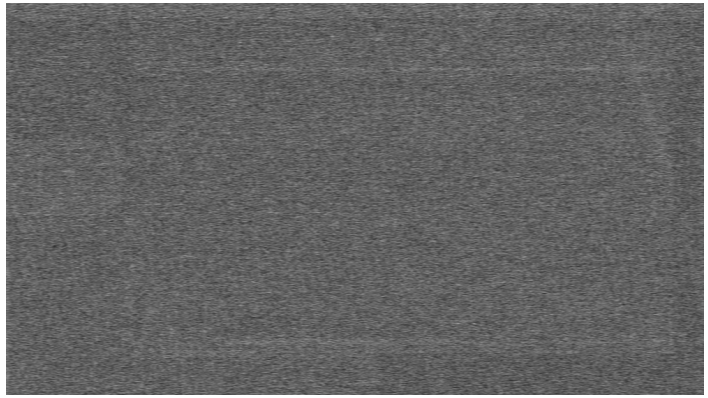
Averaging is easy to improve quality

Leakage amplified by badly shielded connectors

Most risky case: video signal



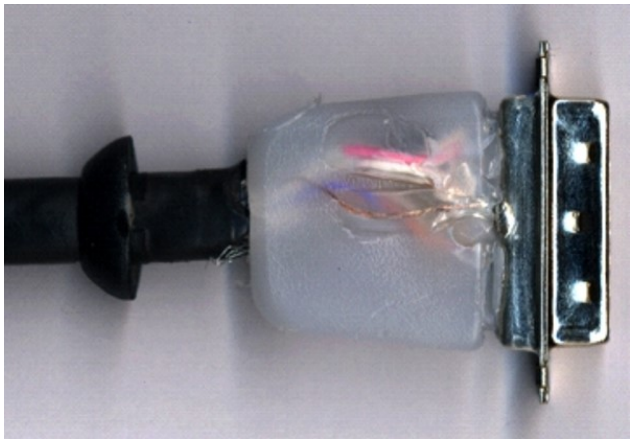
shielded connector



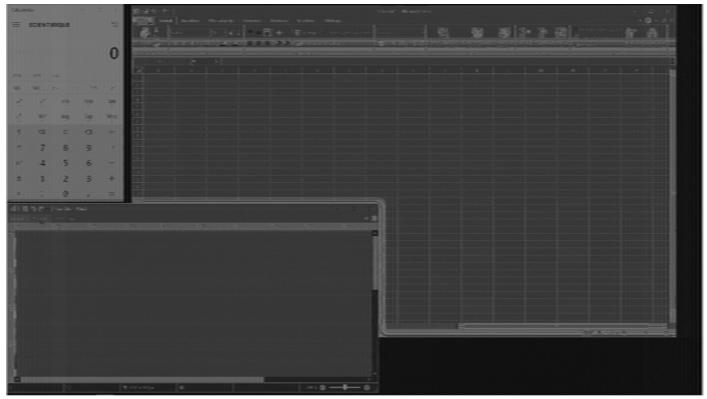
Video signal is repetitive (60 frames/sec)

Averaging is easy to improve quality

Leakage amplified by badly shielded connectors



glued connector



Most risky case: video signal

Most risky case: video signal

VGA

borders only

Most risky case: video signal

VGA

borders only

DVI/HDMI

borders and contrast

Agenda

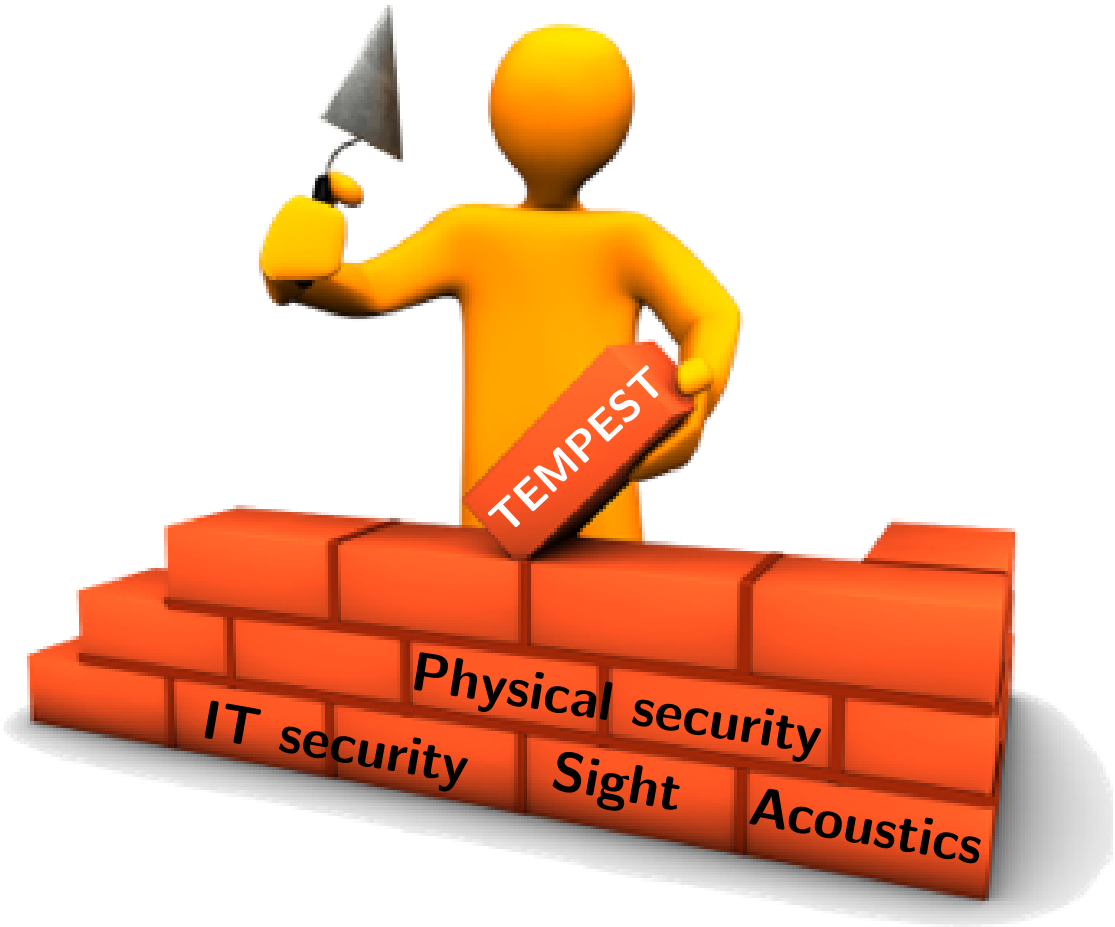
1. The TEMPEST threat
   - Electromagnetic compatibility (EMC)
   - Link between EMC, IT security and TEMPEST
   - Origin of electromagnetic emanations
   - Potential leakage paths
   - Most risky case
2. Protection strategy against electromagnetic emanations
   - Global principle
   - Best protection: shielded enclosure
   - Protection from equipment
   - Protection from building
   - Balanced protection
3. Live demo

Sommaire

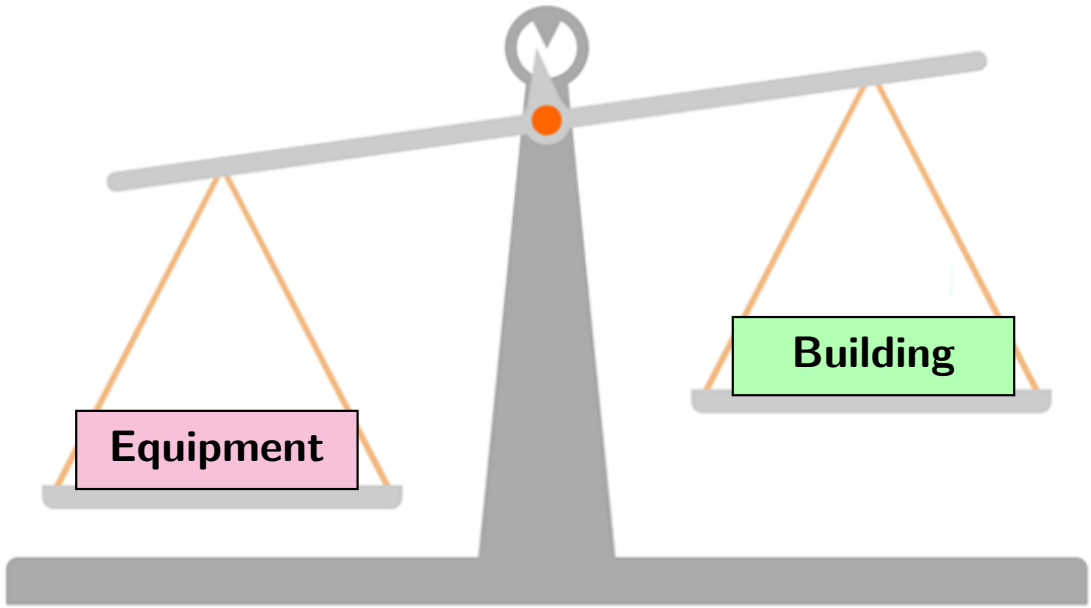
Part of a global protection scheme

Partial protection is not efficient !!!

Part of a global protection scheme

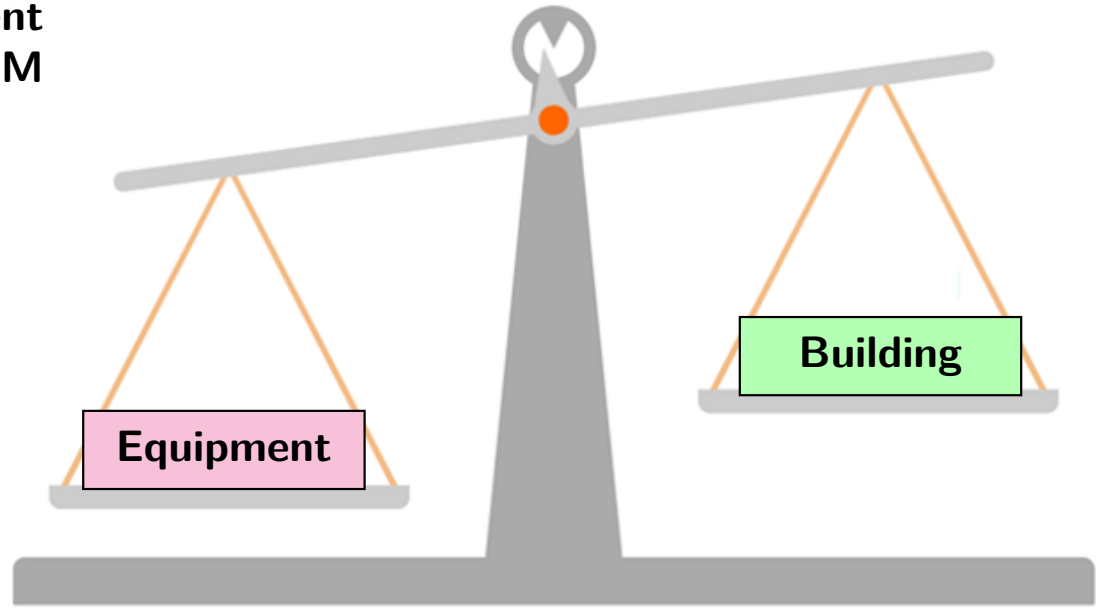


Protection: balance equipment/building

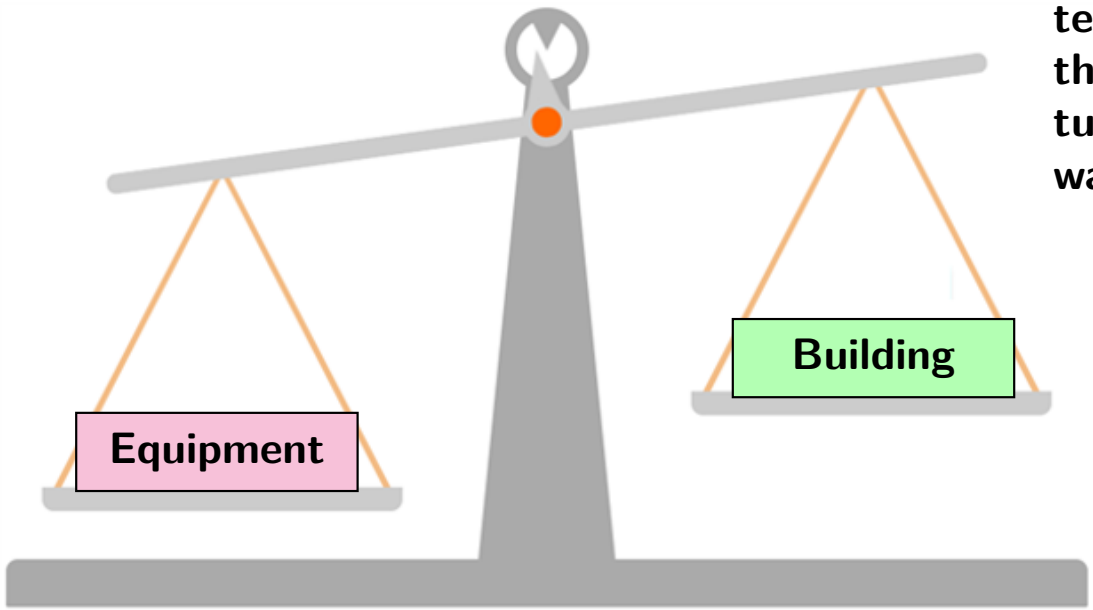


Protection: balance equipment/building

Select equipment with low power EM emanations



Protection: balance equipment/building



Consider the protection given by the building structure face to EM waves

Sommaire

Most efficient protection

Shielded enclosure (or Faraday cage)

Most efficient protection

Shielded enclosure (or Faraday cage)

✓ Best protection

✓ Efficient EM isolation between inside and outside

✓ Typical attenuation: 100 dB within [10 MHz – 1 GHz]

Most efficient protection

Shielded enclosure (or Faraday cage)

✓ Best protection

✓ Efficient EM isolation between inside and outside

✓ Typical attenuation: 100 dB within [10 MHz – 1 GHz]

▲ Door shall stay closed

Most efficient protection

Shielded enclosure (or Faraday cage)

✓ Best protection

✓ Efficient EM isolation between inside and outside

✓ Typical attenuation: 100 dB within [10 MHz – 1 GHz]

▲ Door shall stay closed

✗ Speech not protected

✗ Inefficient against communicating devices

Most efficient protection

Shielded enclosure (or Faraday cage)

✓ Best protection

✓ Efficient EM isolation between inside and outside

✓ Typical attenuation: 100 dB within [10 MHz – 1 GHz]

▲ Door shall stay closed

✗ Speech not protected

➠ Additional acoustic protection

✗ Inefficient against communicating devices

➠ Rise maximum attenuation (140 dB) and freq. (40 GHz)

Most efficient protection

Example: Sistine Chapel was fitted with Faraday cage and electronic jammers to prevent information leak during papal election

But not applicable in all cases

Sommaire

Protection based on equipment selection

?

Level A

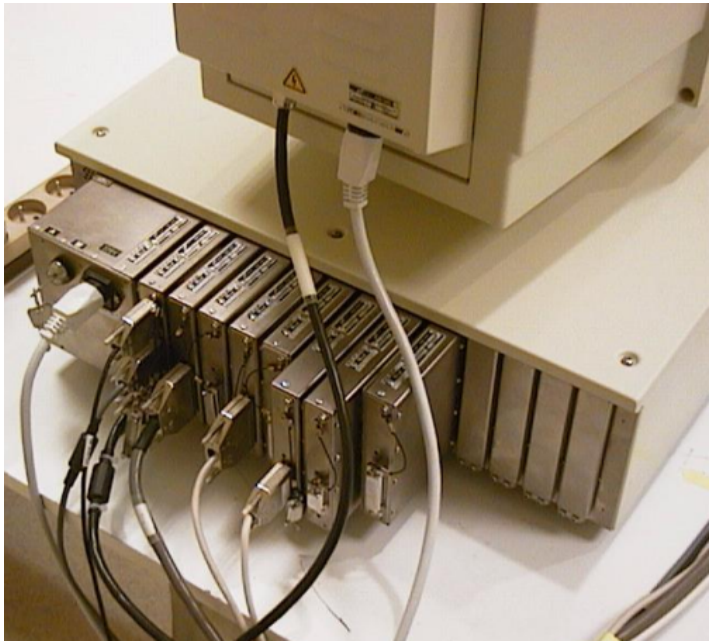
Level B

Level C

Level D

Protection based on equipment selection

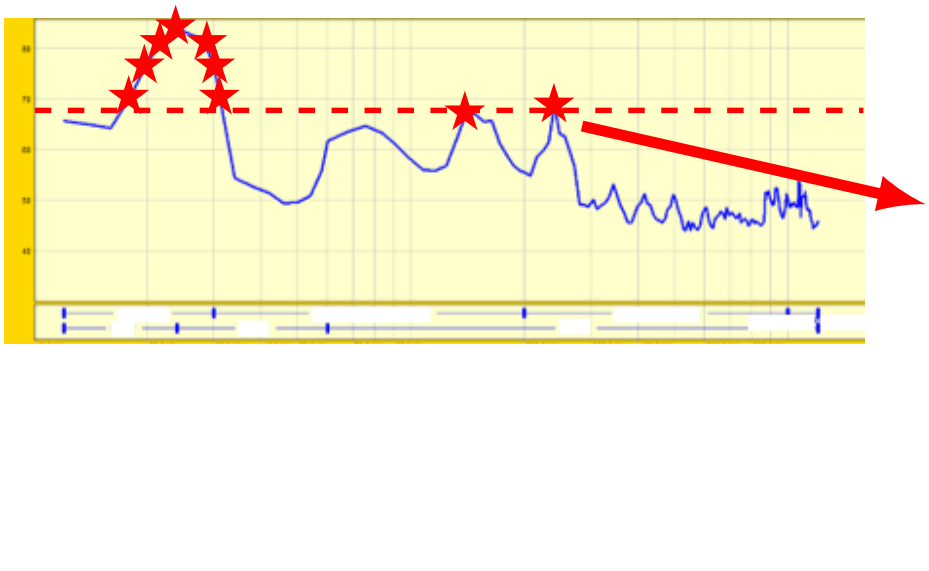
Level A equipment

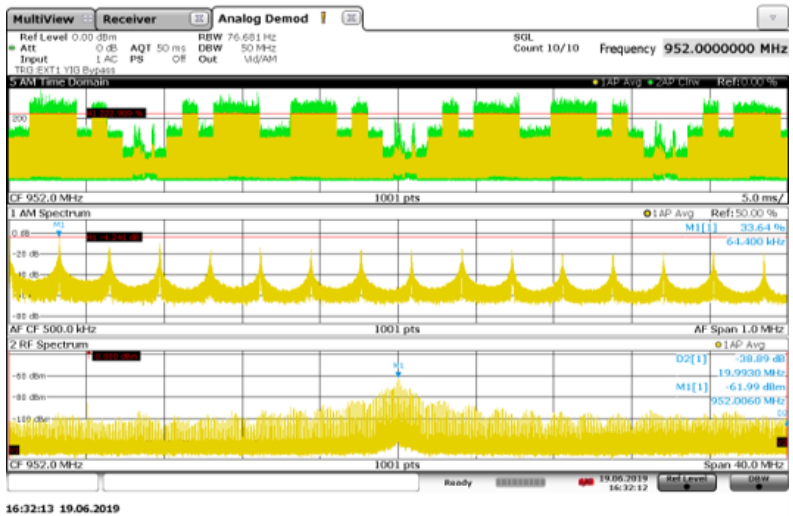


Protection based on equipment selection

Equipment evaluation

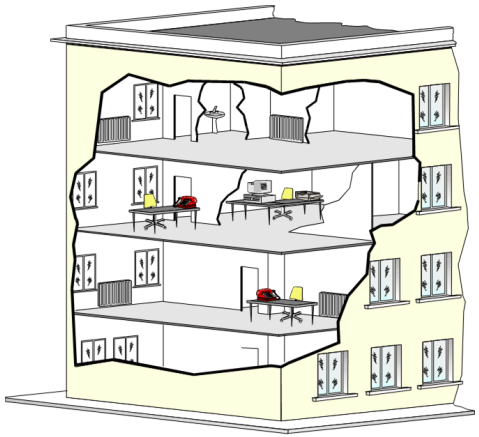
Inside a shielded enclosure to be preserved from EM environment





Sommaire

Protection based on building structure attenuation



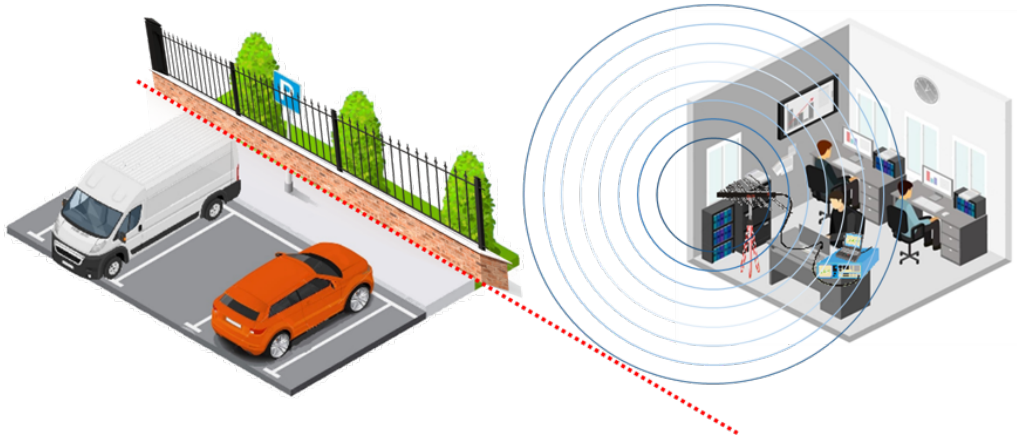
?

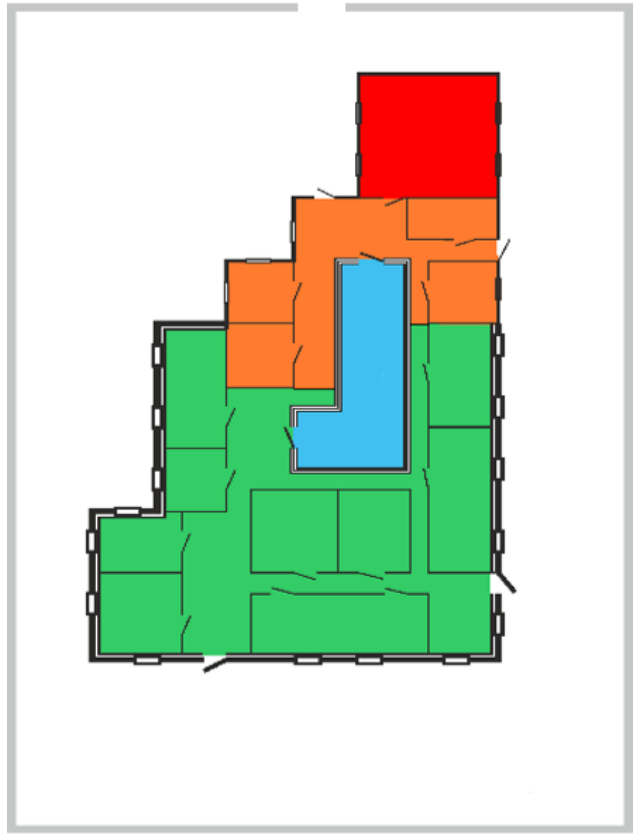
Zone 2

Zone 1

Zone 0

Protection based on building structure attenuation





Sommaire

Association room / equipment

Equipment protection	Room protection
Strong	Strong
Strong	Weak
Weak	Strong
Weak	Weak

Association room / equipment

Equipment protection	Room protection
Strong	Strong
Strong	Weak
Weak	Strong
Weak	Weak

possible leakage

Association room / equipment

Equipment protection	Room protection	
Strong	Strong	additional charge not justified
Strong	Weak	
Weak	Strong	
Weak	Weak	possible leakage

Association room / equipment

Equipment protection	Room protection
Strong	Strong
Strong	Weak
Weak	Strong
Weak	Weak

additional charge not justified

good trade-off, protection level optimized

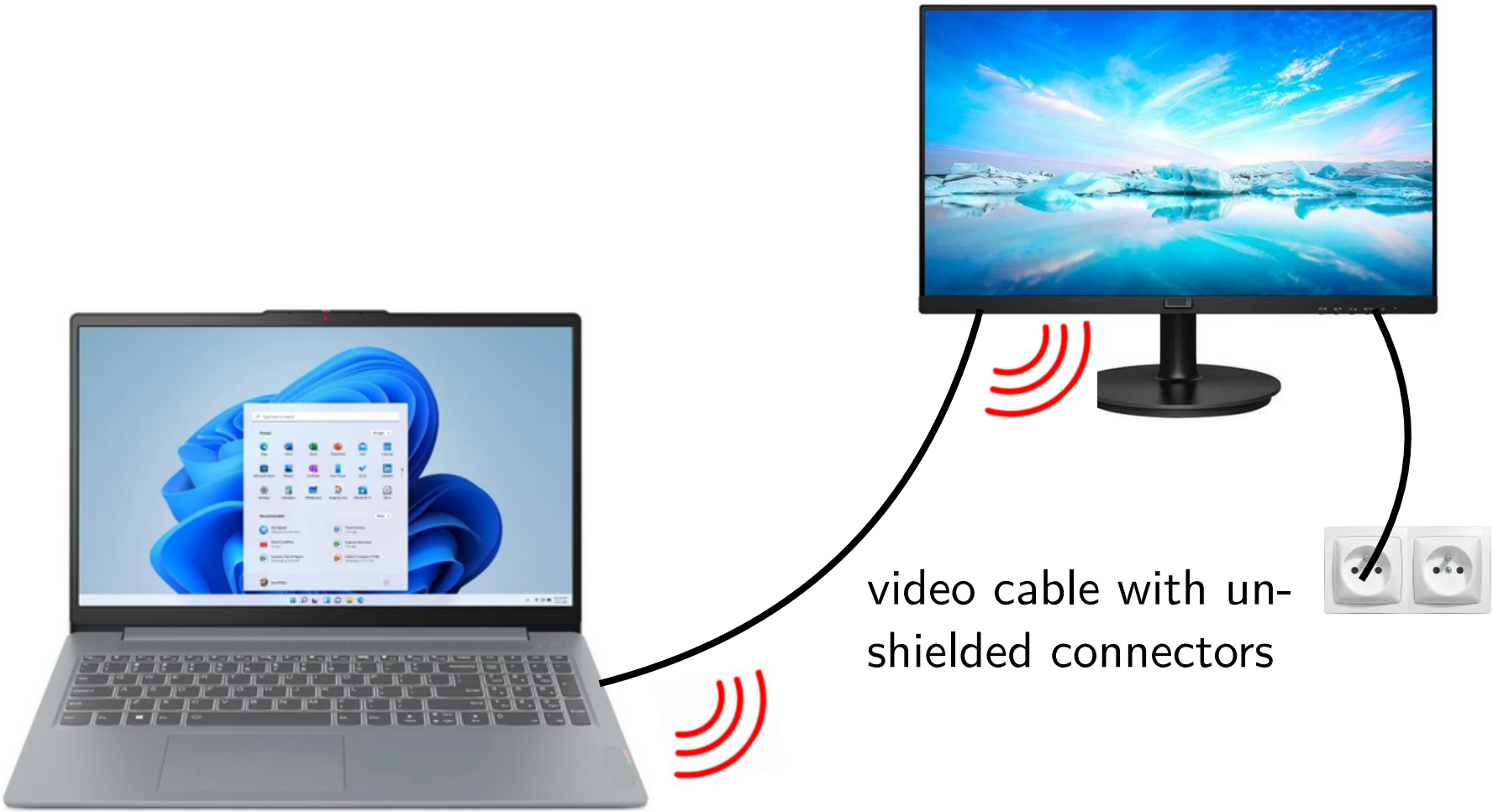
possible leakage

Agenda

1. The TEMPEST threat
   - Electromagnetic compatibility (EMC)
   - Link between EMC, IT security and TEMPEST
   - Origin of electromagnetic emanations
   - Potential leakage paths
   - Most risky case
2. Protection strategy against electromagnetic emanations
   - Global principle
   - Best protection: shielded enclosure
   - Protection from equipment
   - Protection from building
   - Balanced protection
3. Live demo

Demo 1: unshielded video cable

Demo 1: unshielded video cable



Demo 1: receiving chain

Demo 1: receiving chain

Martin Marinov's TempestSDR*

PCB antenna

real-time spectrum analyzer

computer for display

** https://github.com/martinmarinov/TempestSDR*

Demo 2: leakage on power line

Demo 2: leakage on power line

Demo 2: receiving chain

Demo 2: receiving chain

Martin Marinov's TempestSDR*

Current clamp

real-time spectrum analyzer

computer for display

** https://github.com/martinmarinov/TempestSDR*

Thank you for your attention

—

Questions?