Interférences intentionnelles et attaques en faute

différentes similarités

JAIF 21

José Lopes Esteves

LSF, ANSSI

ID

- José Lopes Esteves
- ANSSI – LSF

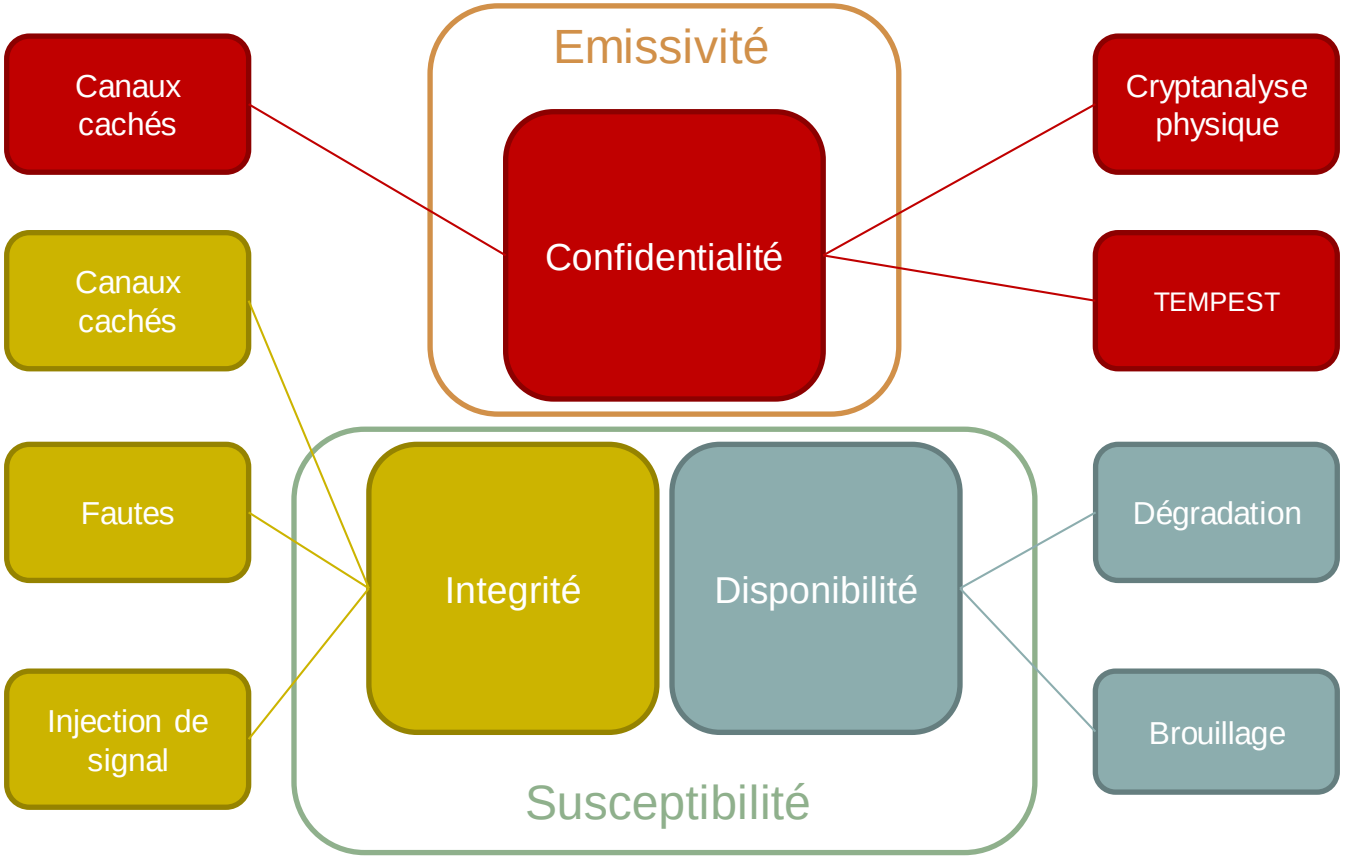
- Sécurité Électromagnétique
- Autorité nationale TEMPEST
- Agressions EM
- Protocoles de radiocommunications

SOMMAIRE

- Interactions EM et SSI
- Interférences intentionnelles et attaques en faute EM
- Projet sonde et coefficient de réflexion
- Conclusion

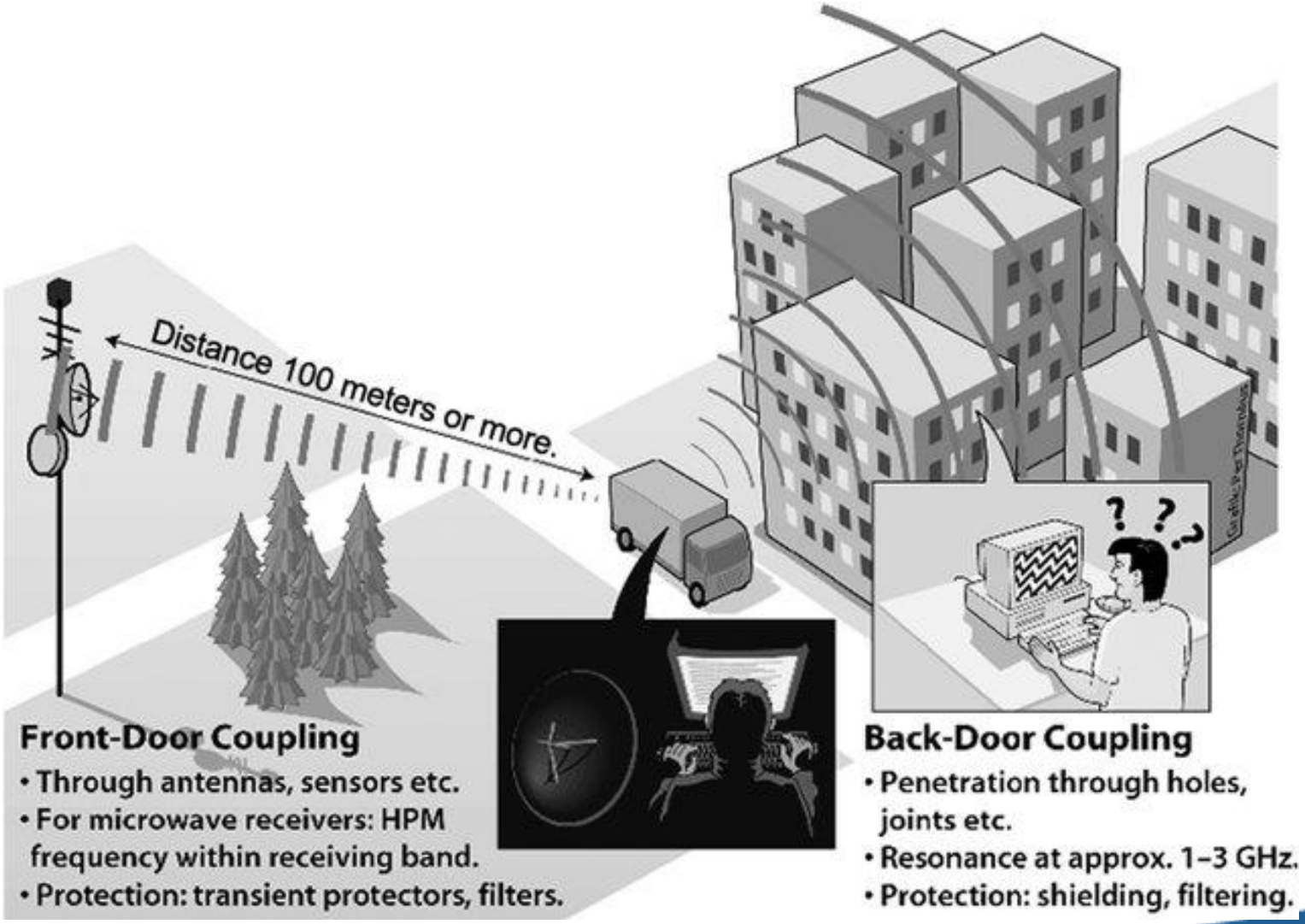
Interactions Electromagnétiques et Sécurité de l'Information

CEM ET SSI


Emissivité
Canaux cachés
Confidentialité
Cryptanalyse physique
TEMPEST
Canaux cachés
Fautes
Integrité
Disponibilité
Dégradation
Injection de signal
Brouillage
Susceptibilité

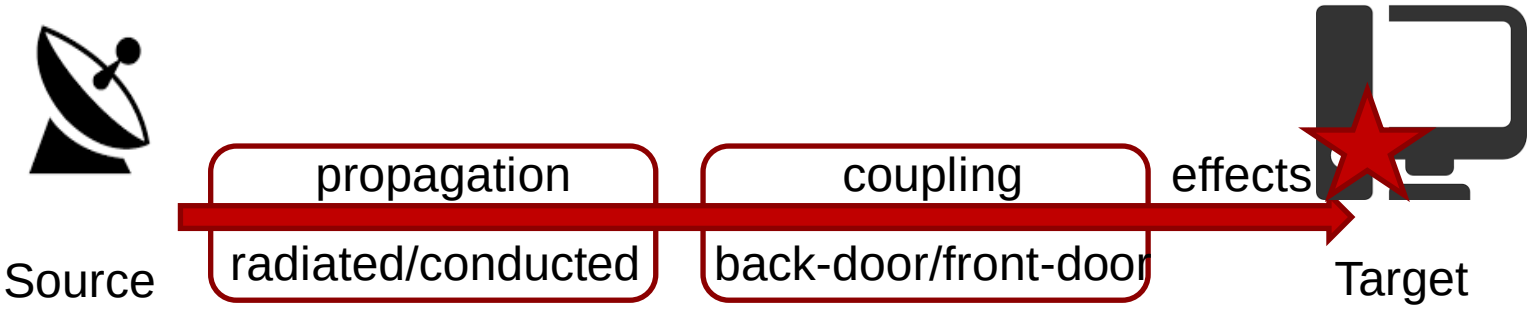
Interférences Intentionnelles et Injection de fautes EM

INTERFÉRENCES INTENTIONNELLES



Backstrom, lovstand, « Susceptibility of electronic systems to high-power microwaves: summary of test exeprience », TEMC46-3

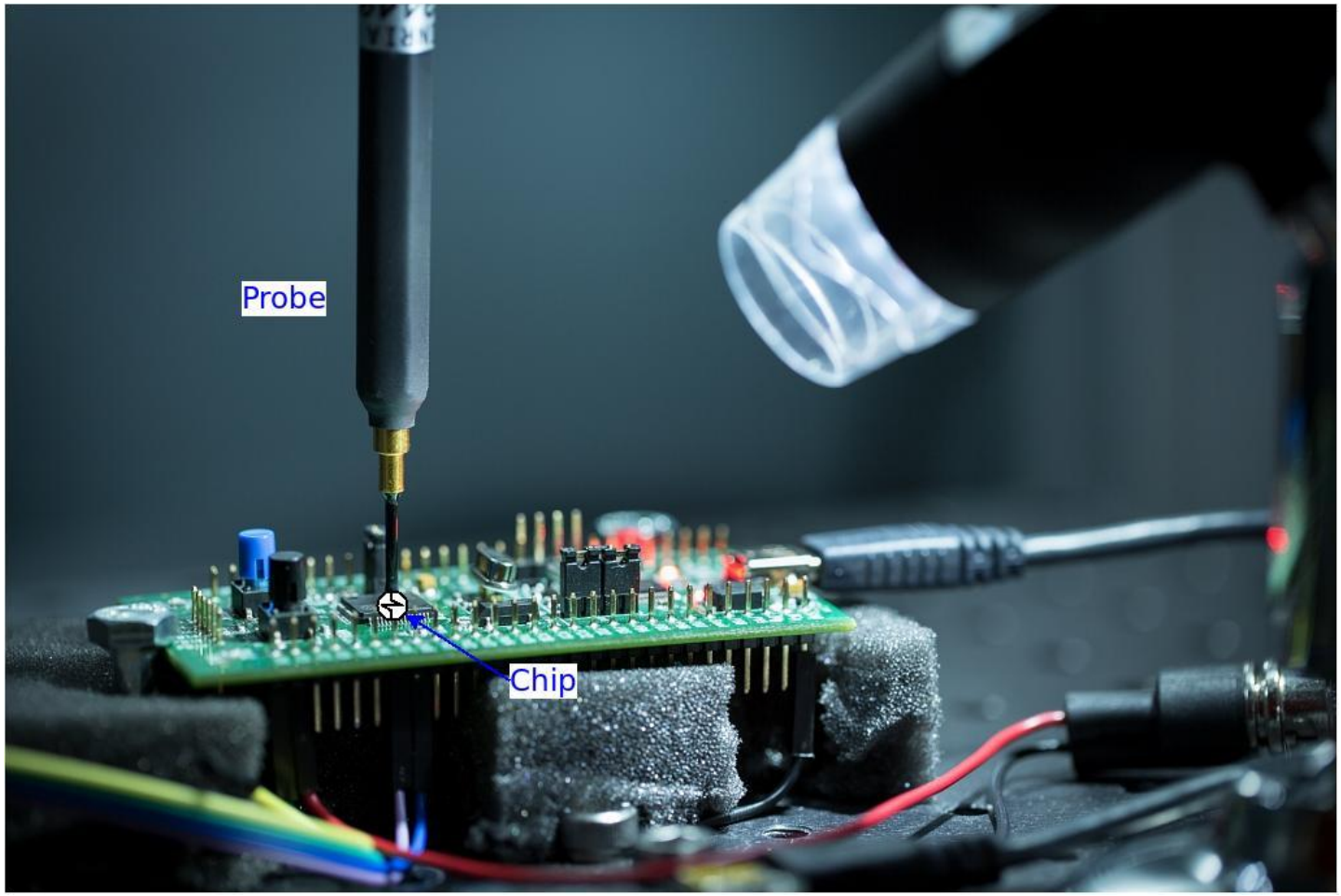
INTERFÉRENCES INTENTIONNELLES



INTERFÉRENCES INTENTIONNELLES

- Menaces en conduction et rayonnement
- Formes d'onde standardisées (ISO 61000)
- Niveaux de puissance élevés
- Attaquant à distance
- Caractérisation effets plutôt axée défaillance
- Du composant au système de systèmes
- Tendance:
  - Formes d'onde plus efficaces
  - Exploitabilité SSI

ATTAQUES EN FAUTE EM



Bukasa, Claudepierre, Lashermes, Lanet, « When fault injection collides with hardware complexity », FPS2018

ATTAQUES EN FAUTE EM

- Propagation conduite: Clock/voltage glitch
- Propagation *rayonnée*: EMFI champ proche
- Accès physique: contrôle et synchro
- Formes d'onde: impulsion et harmonique
- Niveaux: facteur 1 à 100 par rapport à cible
- Cibles: composants
- Caractérisation effets:
  - axée exploitabilité SSI
  - modèles de fautes

POINTS DE CONVERGENCE

- Vers l'analyse d'exploitabilité en IEMI
  - Codes de test
  - Modèles de faute
  - Nouveaux risques
- Vers des fautes à distance via IEMI
  - Equivalences glitch/EMFI
  - Equivalences implusion/CW
  - Nouveaux modèles de menace

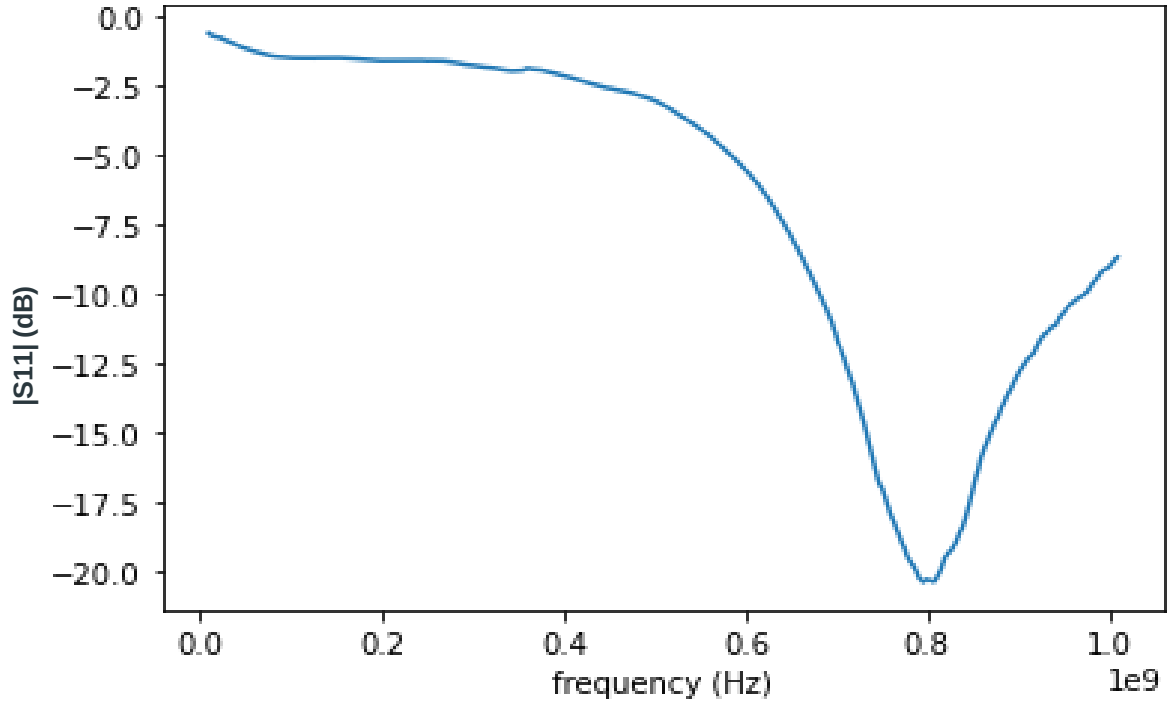
Projet autour des sondes et coefficient de réflexion

SONDE ET S_{11}

- Reproductibilité de l'injection
  - Le fait maison est très tendance
- Détermination du signal transmis
- Caractérisation de la sonde
  - Champ proche complique tout
- Idée:
  - Considérer le couple sonde+cible
  - Regarder le signal non transmis
- Question: le coefficient de réflexion est-il un observable intéressant ?

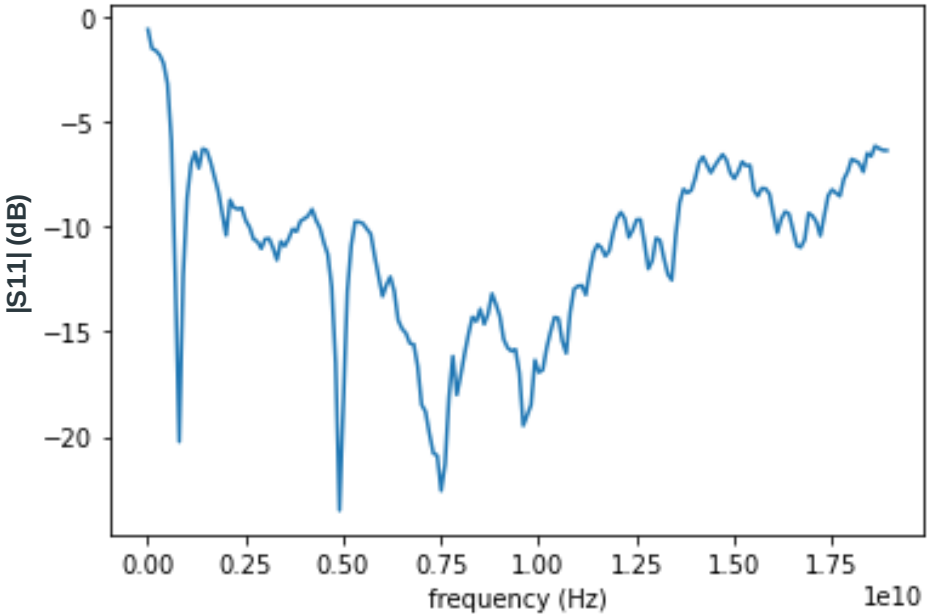
SONDE ET S_{11}

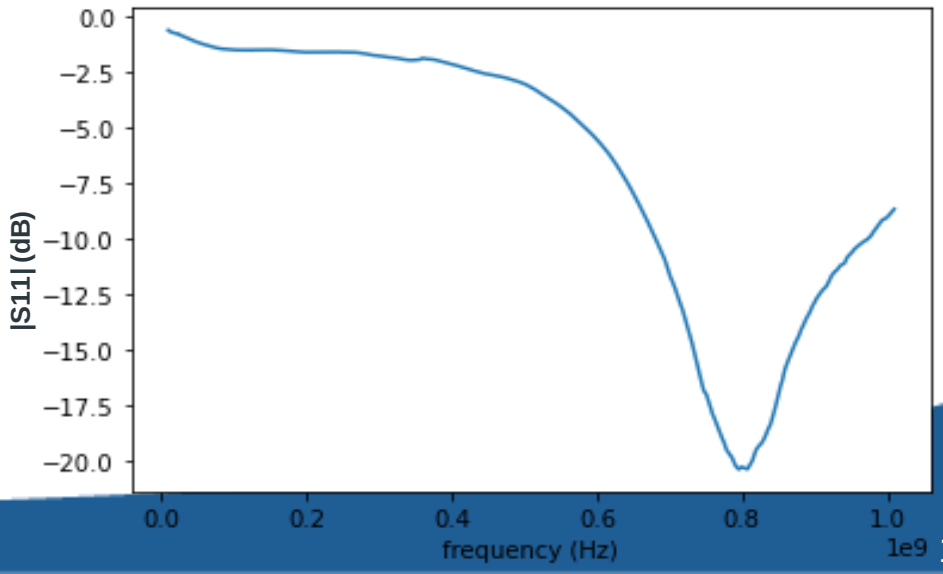
- Coefficient de réflexion (S_{11})
  - Puissance revenant vers la source
  - Pour chaque fréquence



SONDE ET S_{11}: PREMIERS TRAVAUX

- Comparaison carto faute et S_{11}
- Comparaison faute impulsionnelle et harmonique/bande étroite





SONDE ET S_{11}: PERSPECTIVES

- Reproductibilité
  - Adaptation du signal à la source
- Caractérisation
  - Cartographie, points d'injection favorables
  - Impact de l'activité logique
- Profil d'attaquant
  - De l'impulsion à la forme d'onde efficace

Conclusion

CONCLUSION

- IEMI et attaques en faute EM
  - Perturbations via susceptibilité EM
  - Convergence des formes d'onde
  - Modèles de menace complémentaires
- Opportunités pour la caractérisation IEMI
  - Exploitabilité SSI et modèles de faute
- Evolution des modèles de menace
  - Vers une faute à distance
- Reconsidération des profils d'attaquant