

Cybersécurité matérielle: attaque de puces électroniques

Arnaud Tisserand

CNRS, Lab-STICC

Fête de la science, octobre 2017



Introduction

En gros, la **cybersécurité** recouvre tout ce qui porte sur la gestion de la **sécurité** dans le **cyberespace**.

Introduction

En gros, la **cybersécurité** recouvre tout ce qui porte sur la gestion de la **sécurité** dans le **cyberespace**.

Cyberespace : « Espace virtuel rassemblant la communauté des internautes et des ressources d'informations numériques accessibles à travers les réseaux d'ordinateurs » (Petit Larrouse 2015).

Introduction

En gros, la **cybersécurité** recouvre tout ce qui porte sur la gestion de la **sécurité** dans le **cyberespace**.

Cyberespace : « Espace virtuel rassemblant la communauté des internautes et des ressources d'informations numériques accessibles à travers les réseaux d'ordinateurs » (Petit Larrouse 2015).

Cybersécurité :

- lois (politique)

Introduction

En gros, la **cybersécurité** recouvre tout ce qui porte sur la gestion de la **sécurité** dans le **cyberespace**.

Cyberespace : « Espace virtuel rassemblant la communauté des internautes et des ressources d'informations numériques accessibles à travers les réseaux d'ordinateurs » (Petit Larrouse 2015).

Cybersécurité :

- lois (politique)
- concepts et méthodes (théorie)

Introduction

En gros, la **cybersécurité** recouvre tout ce qui porte sur la gestion de la **sécurité** dans le **cyberespace**.

Cyberespace : « Espace virtuel rassemblant la communauté des internautes et des ressources d'informations numériques accessibles à travers les réseaux d'ordinateurs » (Petit Larrouse 2015).

Cybersécurité :

- lois (politique)
- concepts et méthodes (théorie)
- outils et dispositifs (technologie)

Introduction

En gros, la **cybersécurité** recouvre tout ce qui porte sur la gestion de la **sécurité** dans le **cyberespace**.

Cyberespace : « Espace virtuel rassemblant la communauté des internautes et des ressources d'informations numériques accessibles à travers les réseaux d'ordinateurs » (Petit Larrouse 2015).

Cybersécurité :

- lois (politique)
- concepts et méthodes (théorie)
- outils et dispositifs (technologie)
- formations initiales et continues (enseignement)

Introduction

En gros, la **cybersécurité** recouvre tout ce qui porte sur la gestion de la **sécurité** dans le **cyberespace**.

Cyberespace : « Espace virtuel rassemblant la communauté des internautes et des ressources d'informations numériques accessibles à travers les réseaux d'ordinateurs » (Petit Larrouse 2015).

Cybersécurité :

- lois (politique)
- concepts et méthodes (théorie)
- outils et dispositifs (technologie)
- formations initiales et continues (enseignement)
- sensibilisation des citoyens

Introduction

En gros, la **cybersécurité** recouvre tout ce qui porte sur la gestion de la **sécurité** dans le **cyberespace**.

Cyberespace : « Espace virtuel rassemblant la communauté des internautes et des ressources d'informations numériques accessibles à travers les réseaux d'ordinateurs » (Petit Larrouse 2015).

Cybersécurité :

- lois (politique)
- concepts et méthodes (théorie)
- outils et dispositifs (technologie)
- formations initiales et continues (enseignement)
- sensibilisation des citoyens
- à tous les niveaux : personnes, matériels et ce qui est immatériel

Exemples de domaines ayant besoin de cybersécurité



Exemples de domaines ayant besoin de cybersécurité



Exemples de domaines ayant besoin de cybersécurité



Exemples de domaines ayant besoin de cybersécurité



Exemples de domaines ayant besoin de cybersécurité



Exemples de domaines ayant besoin de cybersécurité



Exemples de domaines ayant besoin de cybersécurité

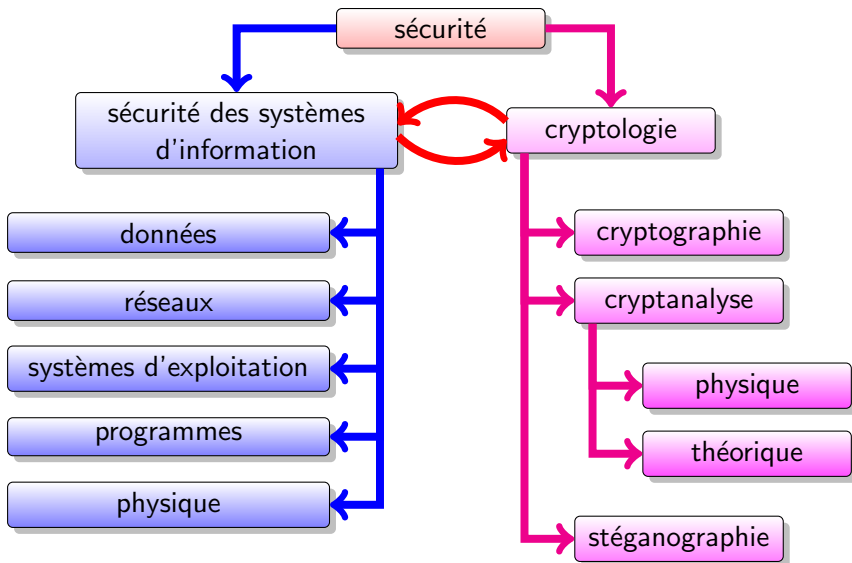


Exemples de domaines ayant besoin de cybersécurité

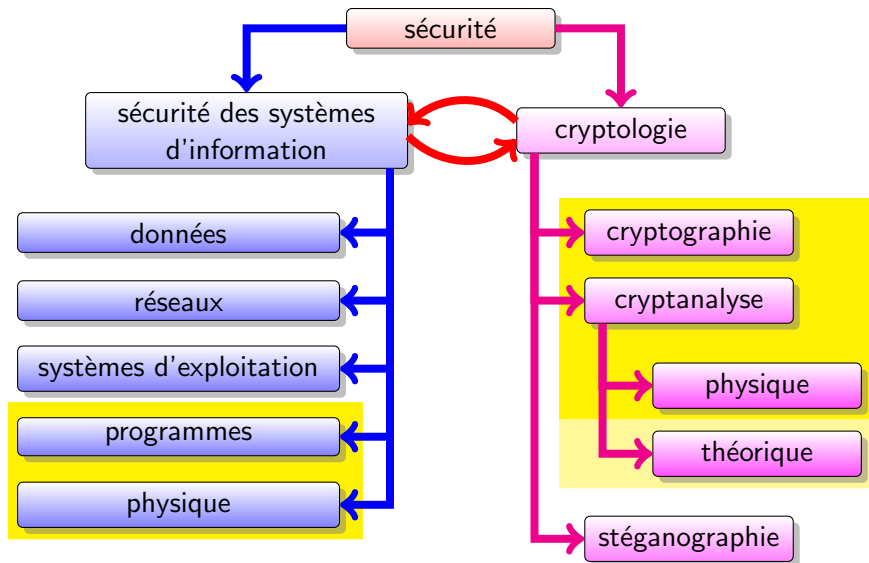


etc. etc. etc.

Sécurité numérique



Sécurité numérique



Un peu de terminologie

Cryptographie : étymologiquement « écriture secrète », méthodes et outils pour rendre les messages incompréhensibles sans avoir la clé

Cryptanalyse : analyse des cryptogrammes pour retrouver les informations secrètes (clé ou message en clair)

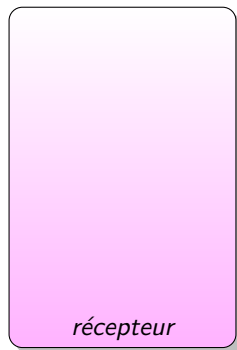
Cryptologie : cryptographie + cryptanalyse

Un peu de terminologie

Cryptographie : étymologiquement « écriture secrète », méthodes et outils pour rendre les messages incompréhensibles sans avoir la clé

Cryptanalyse : analyse des cryptogrammes pour retrouver les informations secrètes (clé ou message en clair)

Cryptologie : cryptographie + cryptanalyse

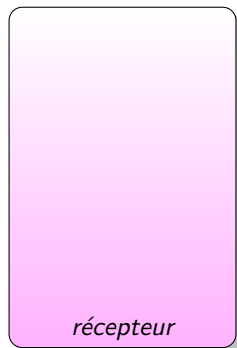
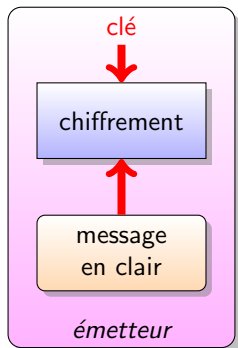


Un peu de terminologie

Cryptographie : étymologiquement « écriture secrète », méthodes et outils pour rendre les messages incompréhensibles sans avoir la clé

Cryptanalyse : analyse des cryptogrammes pour retrouver les informations secrètes (clé ou message en clair)

Cryptologie : cryptographie + cryptanalyse

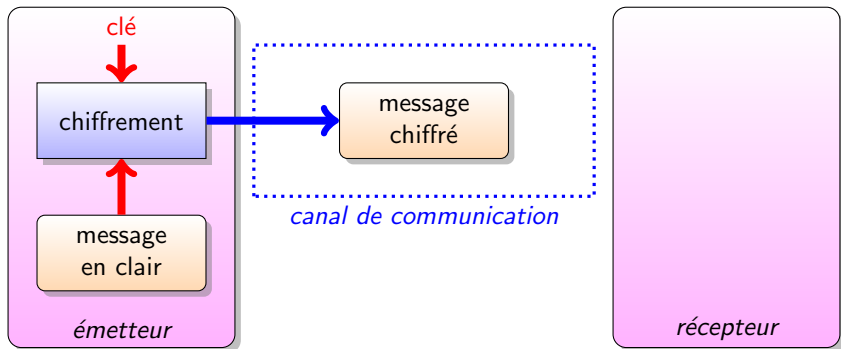


Un peu de terminologie

Cryptographie : étymologiquement « écriture secrète », méthodes et outils pour **rendre les messages incompréhensibles** sans avoir la **clé**

Cryptanalyse : **analyse** des cryptogrammes pour **retrouver** les informations secrètes (clé ou message en clair)

Cryptologie : cryptographie + cryptanalyse

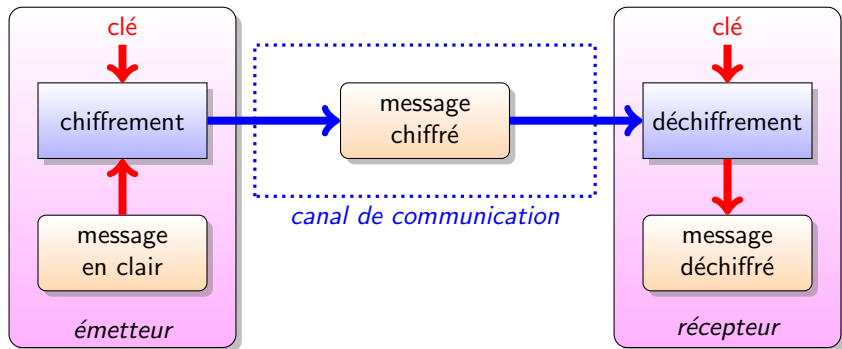


Un peu de terminologie

Cryptographie : étymologiquement « écriture secrète », méthodes et outils pour rendre les messages incompréhensibles sans avoir la clé

Cryptanalyse : analyse des cryptogrammes pour retrouver les informations secrètes (clé ou message en clair)

Cryptologie : cryptographie + cryptanalyse



Analogie avec un coffre et un cadenas



émetteur

récepteur

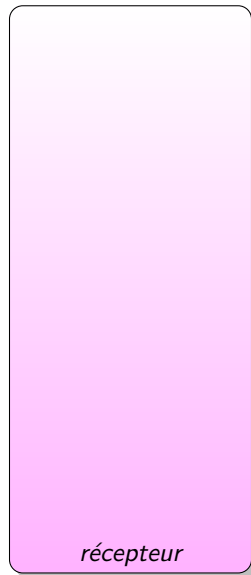
Analogie avec un coffre et un cadenas



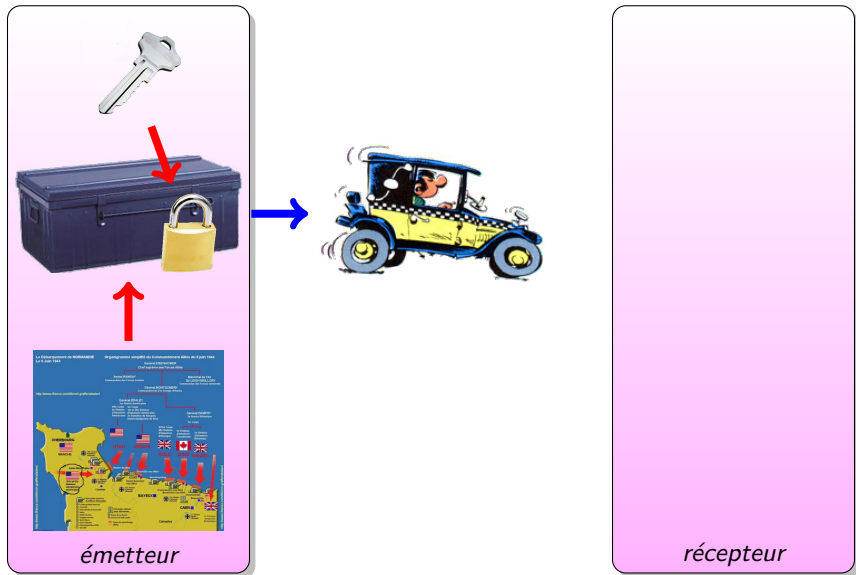
émetteur

récepteur

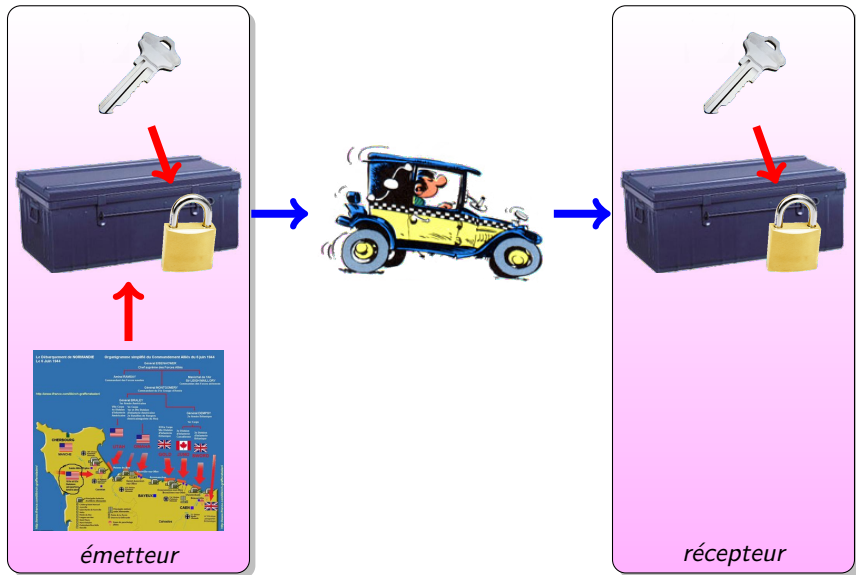
Analogie avec un coffre et un cadenas



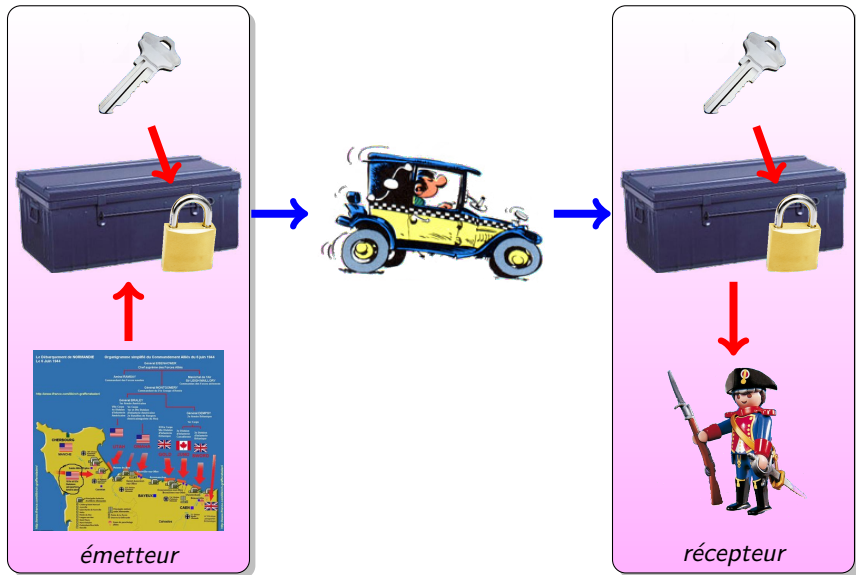
Analogie avec un coffre et un cadenas



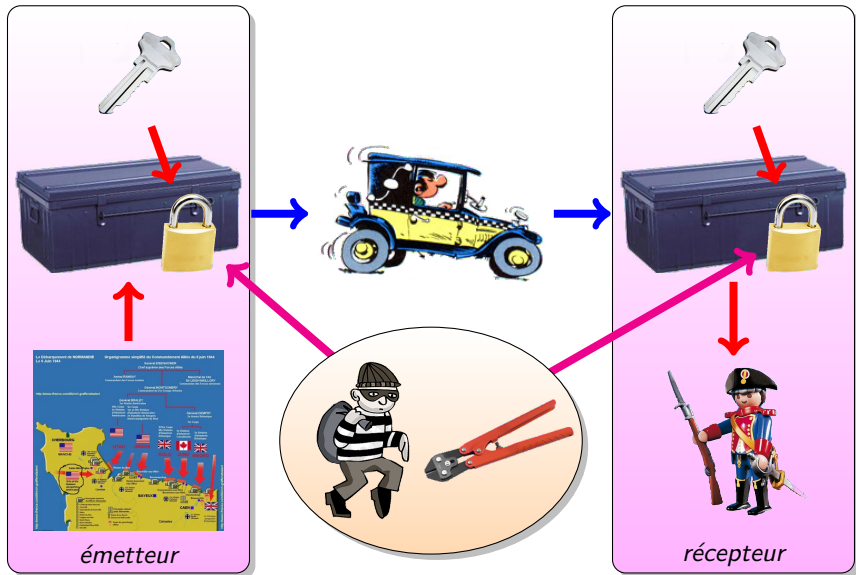
Analogie avec un coffre et un cadenas



Analogie avec un coffre et un cadenas



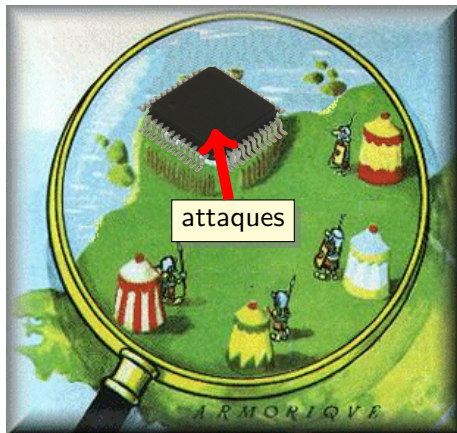
Analogie avec un coffre et un cadenas



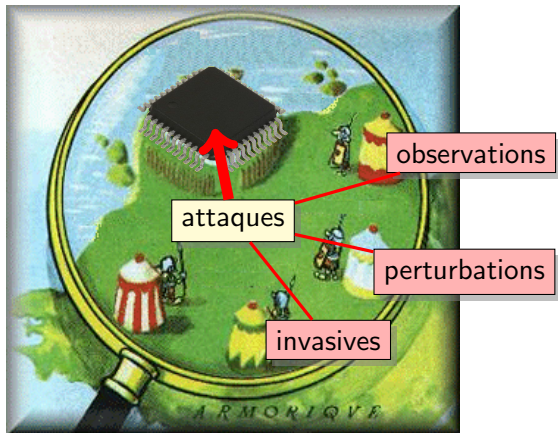
Principaux types d'attaques



Principaux types d'attaques

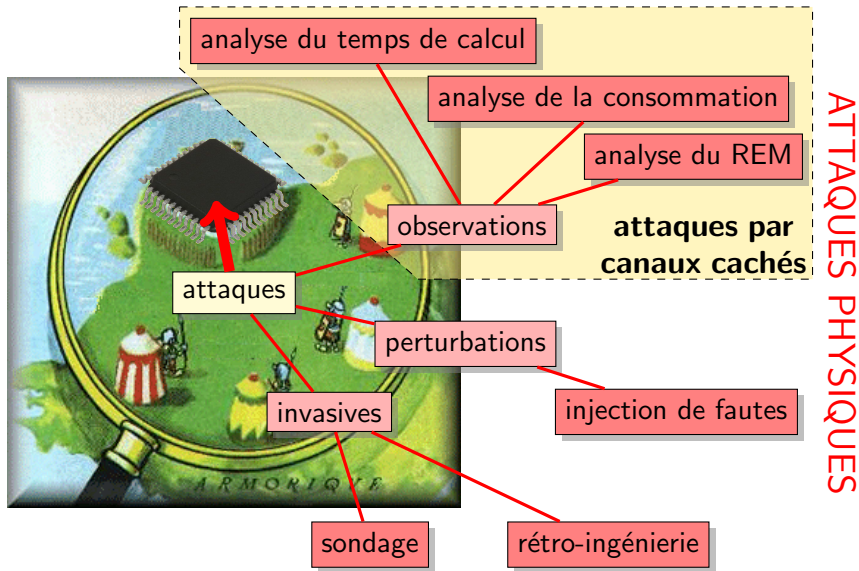


Principaux types d'attaques



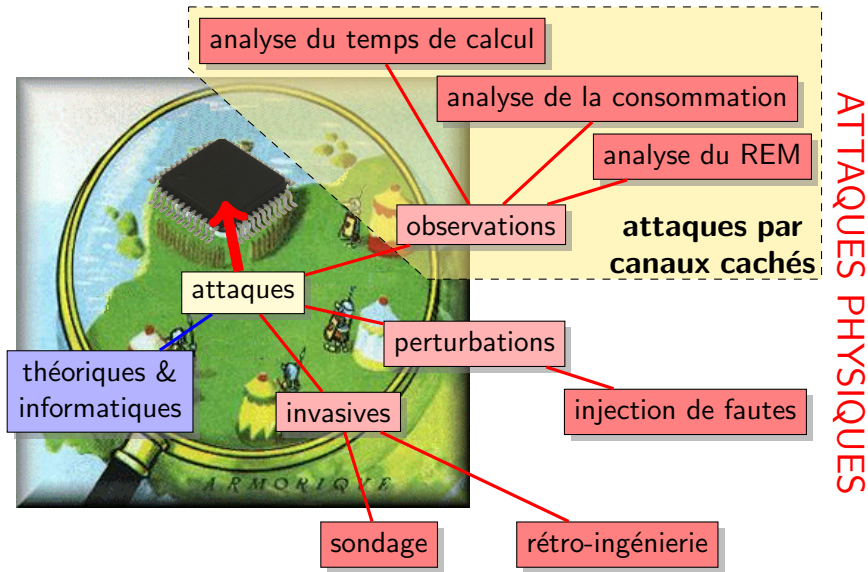
ATTAQUES PHYSIQUES

Principaux types d'attaques



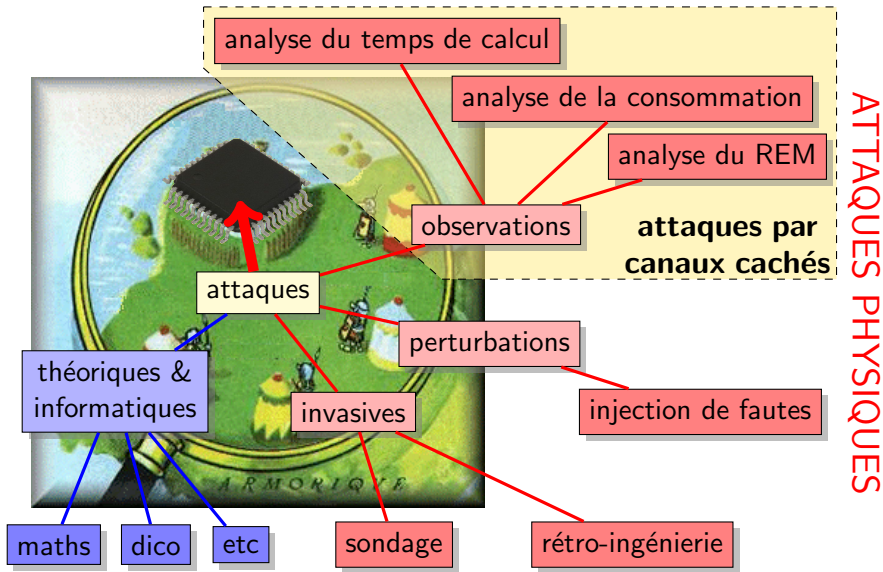
REM = rayonnement électromagnétique

Principaux types d'attaques



REM = rayonnement électromagnétique

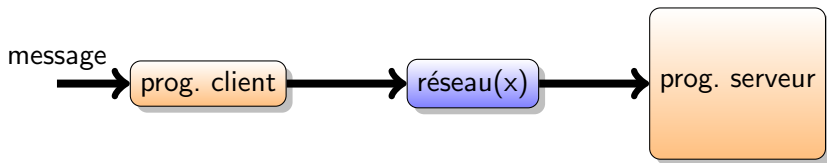
Principaux types d'attaques



REM = rayonnement électromagnétique

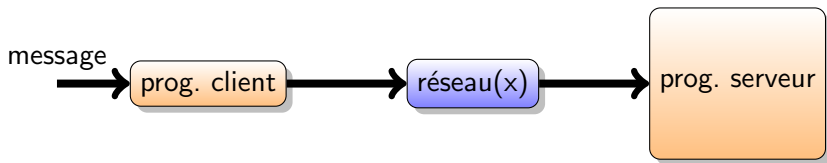
Exemple : Attaque par débordement de tampon

Objectif : détourner le fonctionnement d'un programme (mal fait) de transfert de messages.



Exemple : Attaque par débordement de tampon

Objectif : détourner le fonctionnement d'un programme (mal fait) de transfert de messages.

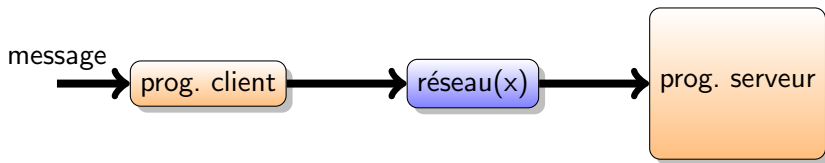


vue de la mémoire du programme sur le serveur :

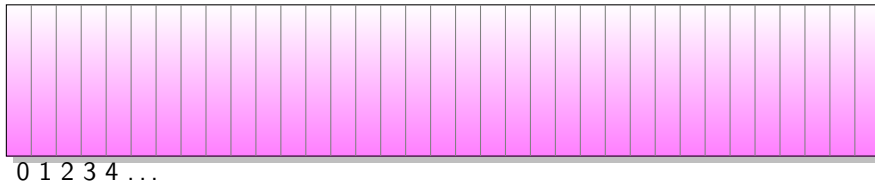


Exemple : Attaque par débordement de tampon

Objectif : détourner le fonctionnement d'un programme (mal fait) de transfert de messages.

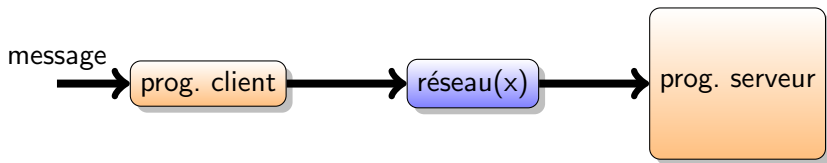


vue de la mémoire du programme sur le serveur :

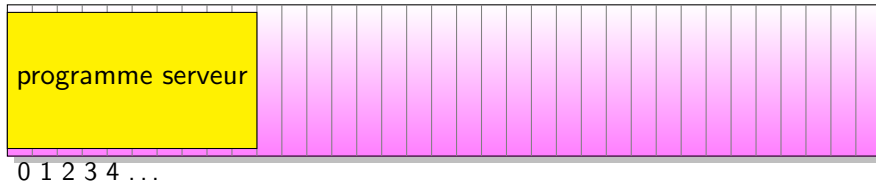


Exemple : Attaque par débordement de tampon

Objectif : détourner le fonctionnement d'un programme (mal fait) de transfert de messages.

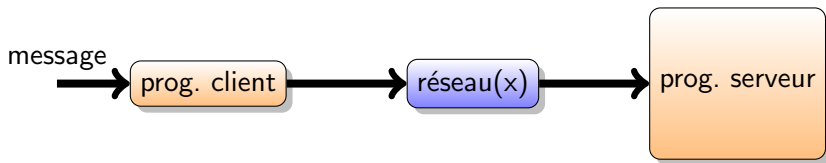


vue de la mémoire du programme sur le serveur :

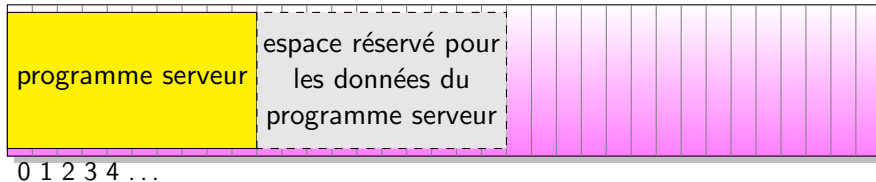


Exemple : Attaque par débordement de tampon

Objectif : détourner le fonctionnement d'un programme (mal fait) de transfert de messages.

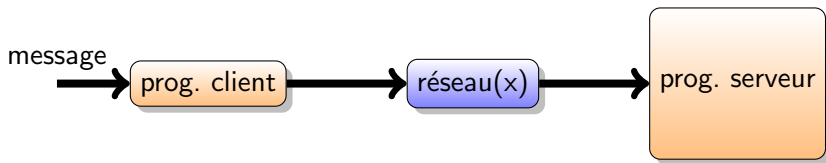


vue de la mémoire du programme sur le serveur :

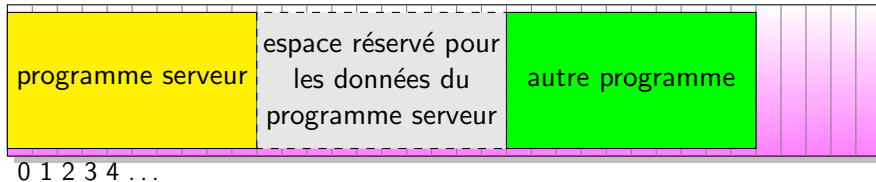


Exemple : Attaque par débordement de tampon

Objectif : détourner le fonctionnement d'un programme (mal fait) de transfert de messages.

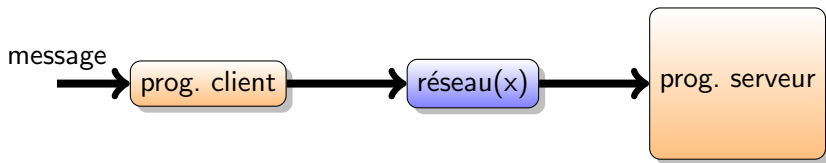


vue de la mémoire du programme sur le serveur :

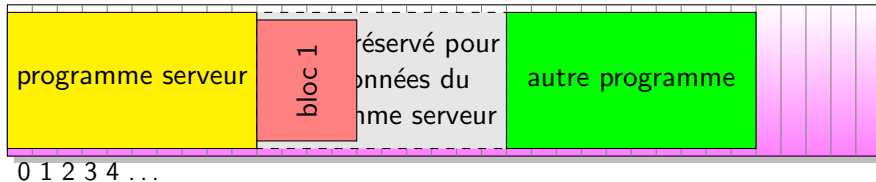


Exemple : Attaque par débordement de tampon

Objectif : détourner le fonctionnement d'un programme (mal fait) de transfert de messages.

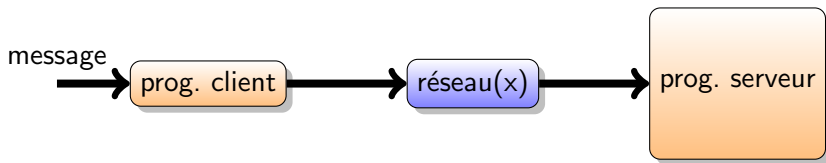


vue de la mémoire du programme sur le serveur :

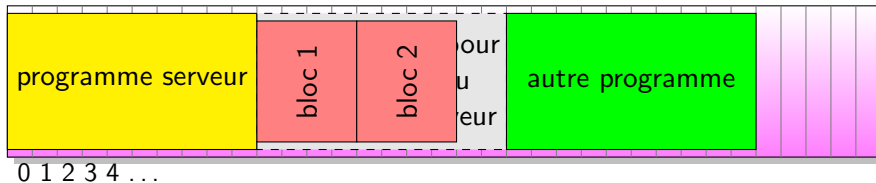


Exemple : Attaque par débordement de tampon

Objectif : détourner le fonctionnement d'un programme (mal fait) de transfert de messages.

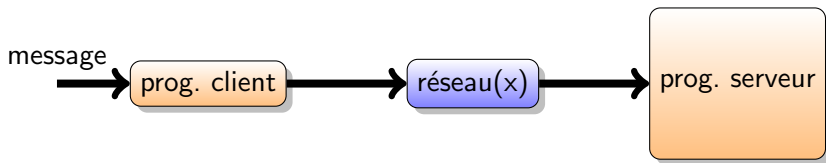


vue de la mémoire du programme sur le serveur :

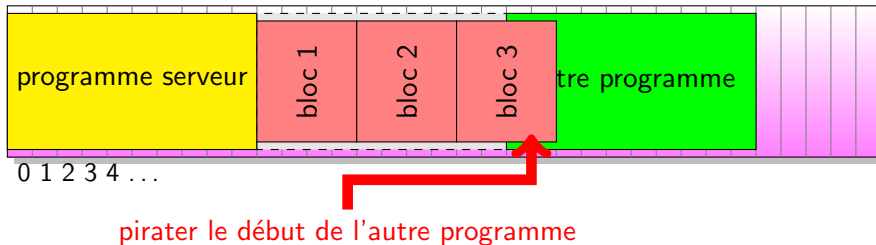


Exemple : Attaque par débordement de tampon

Objectif : détourner le fonctionnement d'un programme (mal fait) de transfert de messages.

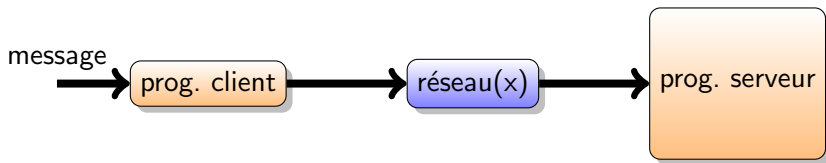


vue de la mémoire du programme sur le serveur :

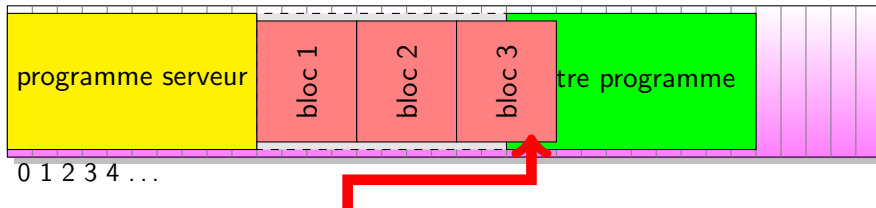


Exemple : Attaque par débordement de tampon

Objectif : détourner le fonctionnement d'un programme (mal fait) de transfert de messages.



vue de la mémoire du programme sur le serveur :



pirater le début de l'autre programme

Protection : ne pas autoriser le débordement (protection mémoire)

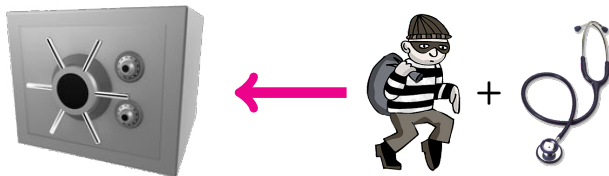
Attaques par canaux cachés, une nouvelle technique ?

Attaques par canaux cachés, une nouvelle technique ?

Pas vraiment ! Vous connaissez tous des attaques par canaux cachés...

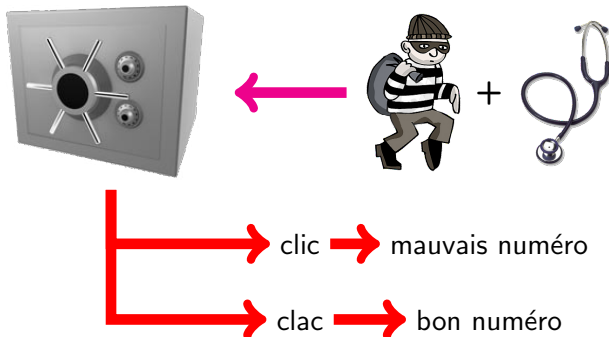
Attaques par canaux cachés, une nouvelle technique ?

Pas vraiment ! Vous connaissez tous des attaques par canaux cachés...



Attaques par canaux cachés, une nouvelle technique ?

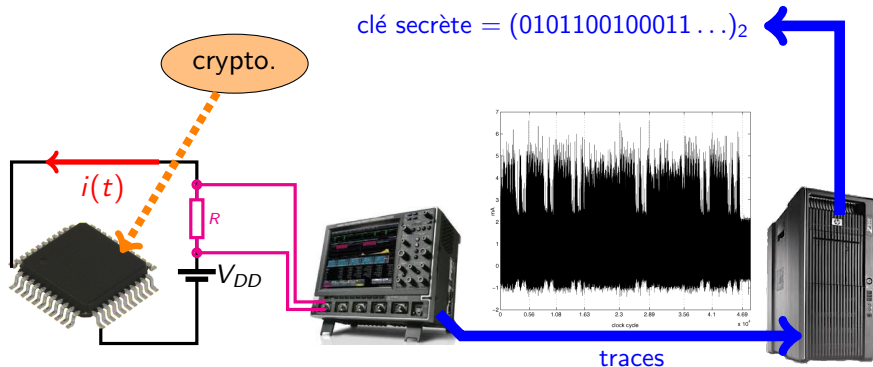
Pas vraiment ! Vous connaissez tous des attaques par canaux cachés...



Attaque par analyse de la consommation d'énergie

Principe général :

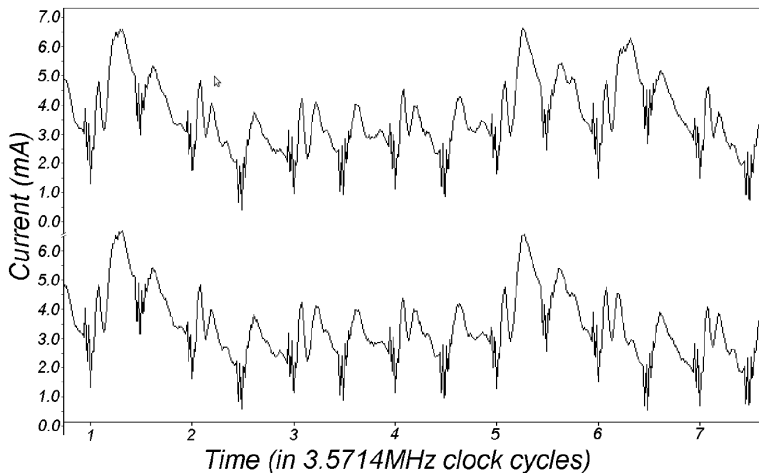
1. mesure du courant $i(t)$ dans le circuit (ou le crypto-système)
2. utiliser ces mesures pour « déduire » des informations secrètes



V_{DD} est la tension d'alimentation du circuit

Analyse simple de la consommation (SPA)

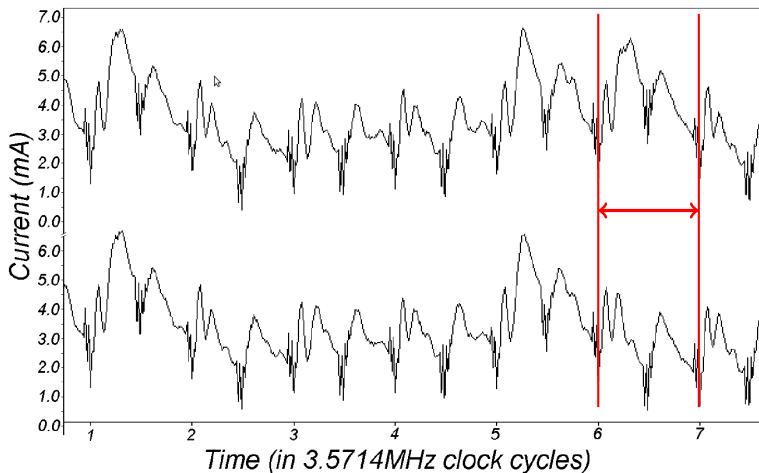
En anglais : SPA *simple power analysis*



Source : article « *Differential Power Analysis* » de P. C. Kocher, J. Jaffe et B. Jun à la conférence CRYPTO-99 (pp. 388-397, DOI : [10.1007/3-540-48405-1_25](https://doi.org/10.1007/3-540-48405-1_25))

Analyse simple de la consommation (SPA)

En anglais : SPA *simple power analysis*



Source : article « *Differential Power Analysis* » de P. C. Kocher, J. Jaffe et B. Jun à la conférence CRYPTO-99 (pp. 388-397, DOI : [10.1007/3-540-48405-1_25](https://doi.org/10.1007/3-540-48405-1_25))

Notre banc d'attaques physiques



Fin, des questions ?

Contact:

- `mailto:arnaud.tisserand@univ-ubs.fr`
- `http://www-labsticc.univ-ubs.fr/~tisseran`
- CNRS, Laboratoire Lab-STICC
Université Bretagne Sud,
Centre de recherche C. Huygens, rue St Maudé, BP 92116,
56321 Lorient cedex, France

Merci