

Cybersécurité et puces électroniques

Arnaud Tisserand

CNRS, Lab-STICC

Fête de la Science, octobre 2017



Préambule

Objectif : présenter une introduction grand public à quelques aspects de la cybersécurité.

Limites : les informations orales et dans ce document peuvent contenir des simplifications, des modifications des sources et ne plus être valides dans le temps (c'est un domaine où les choses changent rapidement).

Sources : indiquées par du texte souligné permettant d'accéder aux liens web (URL) correspondants.

Diffusion : ce document sera disponible publiquement, au format PDF, sur ma page web professionnelle (merci de citer la source).

Terminologie : préfixe cyber

Cybernétique :

- racine grecque proche de : gouvernail, pilote, diriger, gouverner ;
- André-Marie Ampère¹ : art de gouverner les hommes ;
- Norbert Wiener² : contrôle et communications entre les machines et les êtres vivants.

1. 1834 source.

2. 1948, Cybernetics or Control and Communication in the Animal and the Machine.

Terminologie : préfixe cyber

Cybernétique :

- racine grecque proche de : gouvernail, pilote, diriger, gouverner ;
- André-Marie Ampère¹ : art de gouverner les hommes ;
- Norbert Wiener² : contrôle et communications entre les machines et les êtres vivants.

Années 80, le préfixe **cyber** passe dans le vocabulaire courant :

- cyberspace : « Espace virtuel rassemblant la communauté des internautes et des ressources d'informations numériques accessibles à travers les réseaux d'ordinateurs » (Petit Larrouse 2015).
- cybercafé ;
- cybernaute (on utilise plutôt internaute) ;
- cybercommerce (on utilise aussi e-commerce) ;
- ...

1. 1834 source.

2. 1948, Cybernetics or Control and Communication in the Animal and the Machine.

Terminologie : cybersécurité

On trouve de nombreuses définitions, par exemple :

- « Ensemble des procédés informatiques visant à protéger les données transitant par Internet ».

Terminologie : cybersécurité

On trouve de nombreuses définitions, par exemple :

- « Ensemble des procédés informatiques visant à protéger les données transitant par Internet ».
- « État recherché pour un système d'information lui permettant de résister à des événements issus du cyberspace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles ».

Terminologie : cybersécurité

On trouve de nombreuses définitions, par exemple :

- « Ensemble des procédés informatiques visant à protéger les données transitant par Internet ».
- « État recherché pour un système d'information lui permettant de résister à des événements issus du cyberspace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles ».
- « Ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies qui peuvent être utilisés pour protéger les personnes et les actifs informatiques matériels et immatériels (connectés directement ou indirectement à un réseau) des états et des organisations et des personnes ».

Terminologie : cybersécurité aujourd'hui

La cybersécurité recouvre **tout** ce qui porte sur la sécurité dans le cyberspace :

Terminologie : cybersécurité aujourd'hui

La cybersécurité recouvre **tout** ce qui porte sur la sécurité dans le cyberspace :

- lois (politique, compétences dans les tribunaux) ;

Terminologie : cybersécurité aujourd'hui

La **cybersécurité** recouvre **tout** ce qui porte sur la **sécurité** dans le **cyberespace** :

- lois (politique, compétences dans les tribunaux) ;
- concepts et méthodes (aspects théoriques en informatique, électronique, mathématiques, sciences humaines) ;

Terminologie : cybersécurité aujourd'hui

La **cybersécurité** recouvre **tout** ce qui porte sur la **sécurité** dans le **cyberespace** :

- lois (politique, compétences dans les tribunaux) ;
- concepts et méthodes (aspects théoriques en informatique, électronique, mathématiques, sciences humaines) ;
- outils et dispositifs (aspects technologiques) ;

Terminologie : cybersécurité aujourd'hui

La **cybersécurité** recouvre **tout** ce qui porte sur la **sécurité** dans le **cyberespace** :

- lois (politique, compétences dans les tribunaux) ;
- concepts et méthodes (aspects théoriques en informatique, électronique, mathématiques, sciences humaines) ;
- outils et dispositifs (aspects technologiques) ;
- formations initiales et continues (enseignement) ;

Terminologie : cybersécurité aujourd'hui

La **cybersécurité** recouvre **tout** ce qui porte sur la **sécurité** dans le **cyberespace** :

- lois (politique, compétences dans les tribunaux) ;
- concepts et méthodes (aspects théoriques en informatique, électronique, mathématiques, sciences humaines) ;
- outils et dispositifs (aspects technologiques) ;
- formations initiales et continues (enseignement) ;
- sensibilisation des citoyens ;

Terminologie : cybersécurité aujourd'hui

La **cybersécurité** recouvre **tout** ce qui porte sur la **sécurité** dans le **cyberespace** :

- lois (politique, compétences dans les tribunaux) ;
- concepts et méthodes (aspects théoriques en informatique, électronique, mathématiques, sciences humaines) ;
- outils et dispositifs (aspects technologiques) ;
- formations initiales et continues (enseignement) ;
- sensibilisation des citoyens ;
- à tous les niveaux : particuliers, entreprises, administrations, matériels et ce qui est immatériel (programmes, sites web, bases de données, e-services, ...).

Terminologie : autres mots en cyber...

Cyberdéfense : ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberspace les systèmes d'information jugés essentiels.

Cybercriminalité (cybercriminel) : actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.

Cyberdélinquance / cyberdélinquant.

Cyberattaque (cyberattaquant) : acte malveillant envers ou via un dispositif du cyberspace.

Cyberpiratage / cyberespionnage / cybersabotage / cyberharcèlement / cyberintimidation / cyberdignité / cyberterrorisme / ...

Terminologie : attaques

Vulnérabilité : **faiblesse**/**faille** dans un système :

- conception (théorique) ;
- mise en œuvre (pratique) ;
- installation / configuration ;
- exploitation / utilisation.

DCP 198x

PSN 2011

MDP par défaut

MDP sur post-it

Terminologie : attaques

Vulnérabilité : **faiblesse**/**faille** dans un système :

- conception (théorique) ; DCP 198x
- mise en œuvre (pratique) ; PSN 2011
- installation / configuration ; MDP par défaut
- exploitation / utilisation. MDP sur post-it

Menace : cause *potentielle* d'un incident qui pourrait entraîner des dommages si la menace se concrétise, ou attaquant.

Terminologie : attaques

Vulnérabilité : *faiblesse/faille* dans un système :

- conception (théorique) ; DCP 198x
- mise en œuvre (pratique) ; PSN 2011
- installation / configuration ; MDP par défaut
- exploitation / utilisation. MDP sur post-it

Menace : cause *potentielle* d'un incident qui pourrait entraîner des dommages si la menace se concrétise, ou attaquant.

Attaque : *méthode* pour *exploiter concrètement* une vulnérabilité.

Terminologie : attaques

Vulnérabilité : **faiblesse**/**faille** dans un système :

- conception (théorique) ; DCP 198x
- mise en œuvre (pratique) ; PSN 2011
- installation / configuration ; MDP par défaut
- exploitation / utilisation. MDP sur post-it

Menace : cause *potentielle* d'un incident qui pourrait entraîner des dommages si la menace se concrétise, ou attaquant.

Attaque : **méthode** pour **exploiter concrètement** une vulnérabilité.

Protection ou **contre-mesure** : méthode ou dispositif qui **contre** une attaque ou qui **supprime**/**limite** une vulnérabilité

Menaces typiques

- Utilisateurs étourdis/insouciants.
 - Sinistre : vol, inondation, incendie, ...
 - Programmes malveillants : virus, vers, trojan, ...
 - Personnes/groupes malveillants :
 - ▶ « bidouilleur » ;
 - ▶ *hacker(s)* chevronné(s) ;
 - ▶ société concurrente ;
 - ▶ mafia ;
 - ▶ gouvernement.
- 
- puissance d'attaque

Sécurité et sûreté

Attention, selon les contextes, ces mots ont des significations différentes :

- protection contre des risques naturels (pannes, accidents, aléas climatiques, ...).
- protection contre des risques non naturels (malveillance, sabotage, attaques, ...);

Sécurité et sûreté

Attention, selon les contextes, ces mots ont des significations différentes :

- protection contre des risques naturels (pannes, accidents, aléas climatiques, ...).
- protection contre des risques non naturels (malveillance, sabotage, attaques, ...);

Souvent en anglais : *safety* = sécurité et *security* = sûreté.

Sécurité et sûreté

Attention, selon les contextes, ces mots ont des significations différentes :

- protection contre des risques naturels (pannes, accidents, aléas climatiques, ...).
- protection contre des risques non naturels (malveillance, sabotage, attaques, ...);

Souvent en anglais : *safety* = sécurité et *security* = sûreté.

En cybersécurité, on s'occupe du caractère malveillant (pas des pannes).

Quelques estimations

Victimes de cyberattaques³ : 12 **personnes / s.**

Étude auprès de 70 organisations dans 61 pays⁴ : il faut quelques **minutes** pour compromettre la sécurité de données importantes.

Estimation⁵ du coût annuel des cyberattaques sur les entreprises $400 \cdot 10^9$ \$ dans le monde.

Emploi : différentes estimations évaluent à plusieurs **centaines de milliers d'emplois perdus** chaque année en Europe du fait de la cybercriminalité.

3. Source : Microsoft Secure Blog, 27 janvier 2016.

4. Source : Verizon Data Breach Investigation Report 2015.

5. Source : Fortune: interview CEO Lloyd's en janvier 2015.

Exemples de domaines ayant besoin de cybersécurité



etc. etc. etc.

Sources : NASA, Google, SNCF, Airbus, Orange, MinDef, Franquin, etc.

Exemples de domaines ayant besoin de cybersécurité



etc. etc. etc.

Sources : NASA, Google, SNCF, Airbus, Orange, MinDef, Franquin, etc.

Exemples de domaines ayant besoin de cybersécurité



etc. etc. etc.

Sources : NASA, Google, SNCF, Airbus, Orange, MinDef, Franquin, etc.

Exemples de domaines ayant besoin de cybersécurité



etc. etc. etc.

Sources : NASA, Google, SNCF, Airbus, Orange, MinDef, Franquin, etc.

Exemples de domaines ayant besoin de cybersécurité



etc. etc. etc.

Sources : NASA, Google, SNCF, Airbus, Orange, MinDef, Franquin, etc.

Exemples de domaines ayant besoin de cybersécurité



etc. etc. etc.

Sources : NASA, Google, SNCF, Airbus, Orange, MinDef, Franquin, etc.

Exemples de domaines ayant besoin de cybersécurité

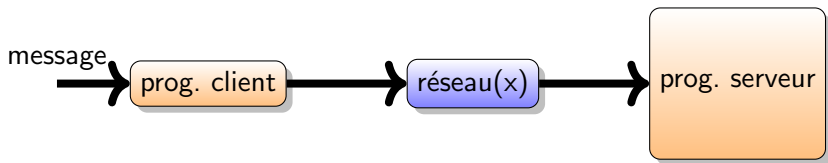


etc. etc. etc.

Sources : NASA, Google, SNCF, Airbus, Orange, MinDef, Franquin, etc.

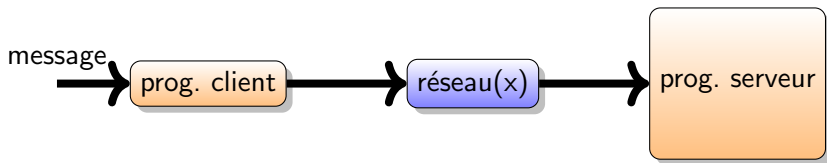
Attaque par débordement de la mémoire

Objectif : détourner le fonctionnement d'un programme (mal fait) pour modifier le programme cible de l'attaque.



Attaque par débordement de la mémoire

Objectif : détourner le fonctionnement d'un programme (mal fait) pour modifier le programme cible de l'attaque.

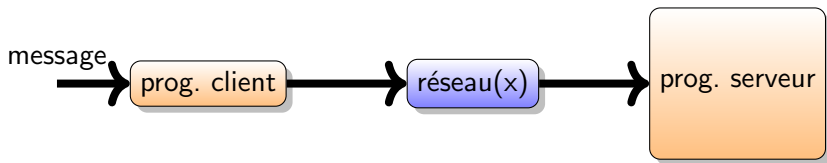


vue de la mémoire du programme sur le serveur :

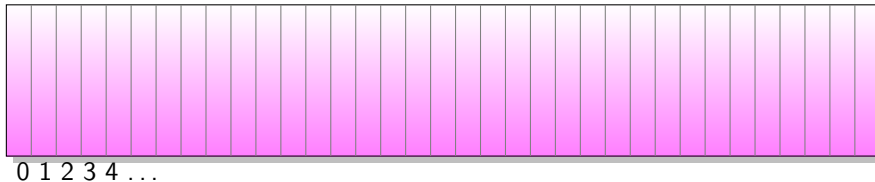


Attaque par débordement de la mémoire

Objectif : détourner le fonctionnement d'un programme (mal fait) pour modifier le programme cible de l'attaque.

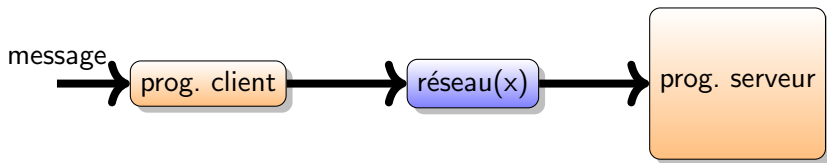


vue de la mémoire du programme sur le serveur :

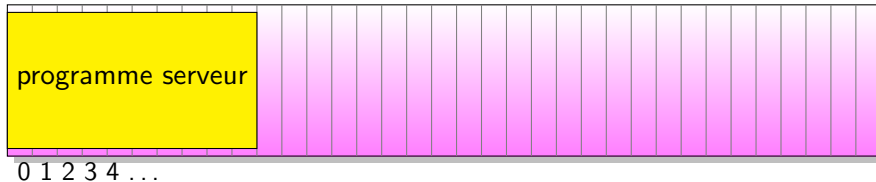


Attaque par débordement de la mémoire

Objectif : détourner le fonctionnement d'un programme (mal fait) pour modifier le programme cible de l'attaque.

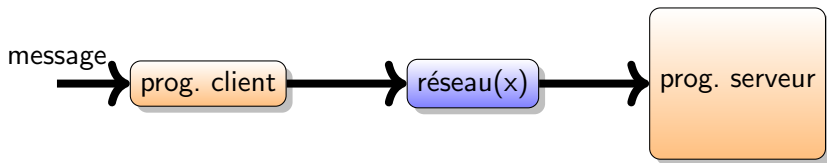


vue de la mémoire du programme sur le serveur :

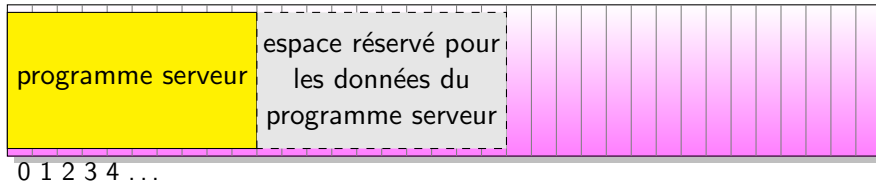


Attaque par débordement de la mémoire

Objectif : détourner le fonctionnement d'un programme (mal fait) pour modifier le programme cible de l'attaque.

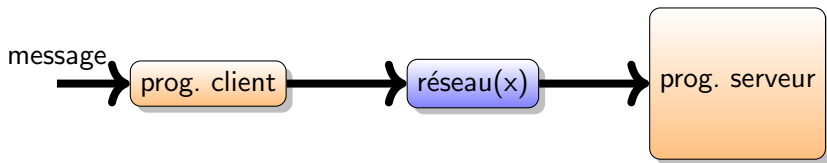


vue de la mémoire du programme sur le serveur :

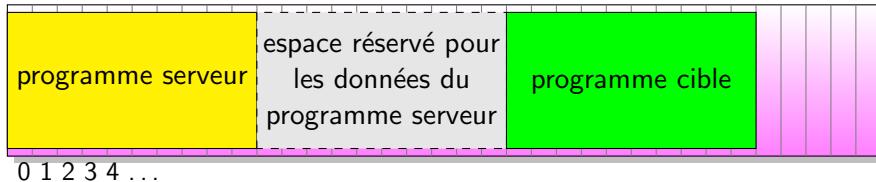


Attaque par débordement de la mémoire

Objectif : détourner le fonctionnement d'un programme (mal fait) pour modifier le programme cible de l'attaque.

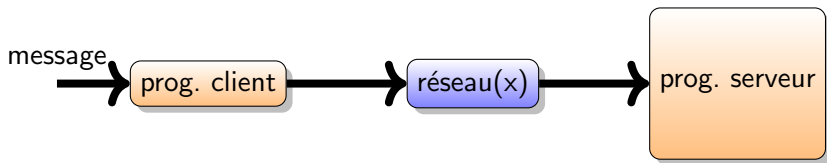


vue de la mémoire du programme sur le serveur :

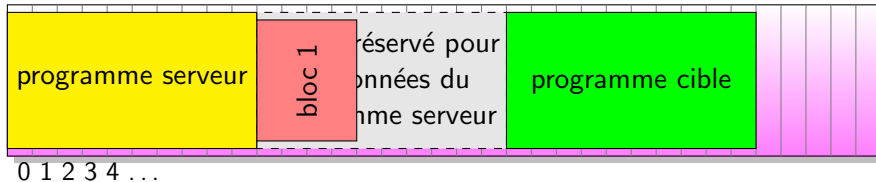


Attaque par débordement de la mémoire

Objectif : détourner le fonctionnement d'un programme (mal fait) pour modifier le programme cible de l'attaque.

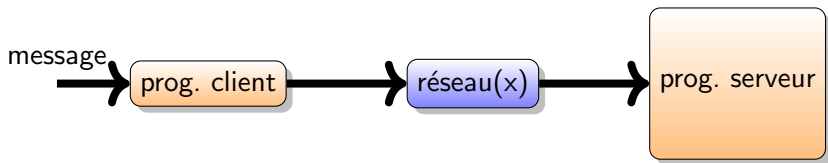


vue de la mémoire du programme sur le serveur :

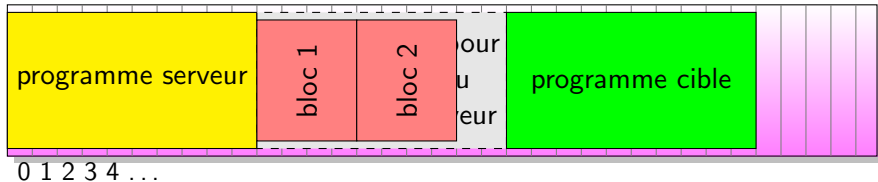


Attaque par débordement de la mémoire

Objectif : détourner le fonctionnement d'un programme (mal fait) pour modifier le programme cible de l'attaque.

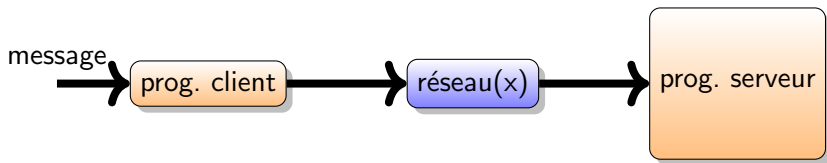


vue de la mémoire du programme sur le serveur :

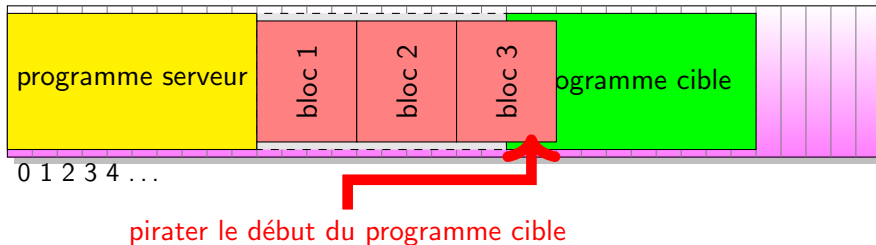


Attaque par débordement de la mémoire

Objectif : détourner le fonctionnement d'un programme (mal fait) pour modifier le programme cible de l'attaque.

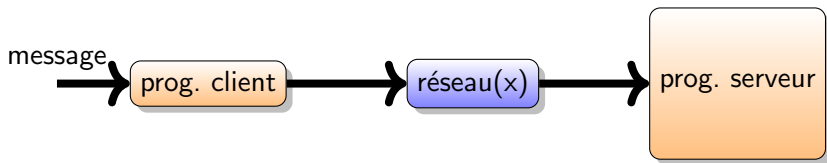


vue de la mémoire du programme sur le serveur :

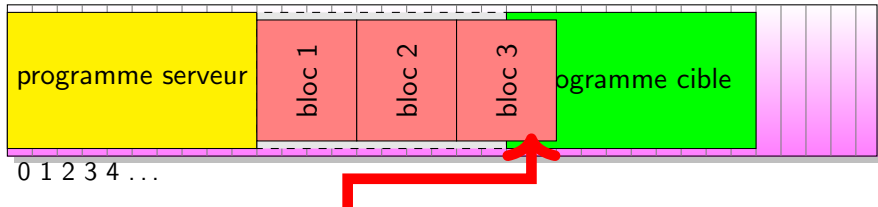


Attaque par débordement de la mémoire

Objectif : détourner le fonctionnement d'un programme (mal fait) pour modifier le programme cible de l'attaque.



vue de la mémoire du programme sur le serveur :



pirater le début du programme cible

Protection : ne pas autoriser le débordement (protection mémoire)

Attaques par relais

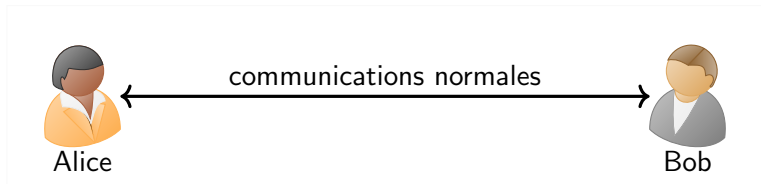


Alice

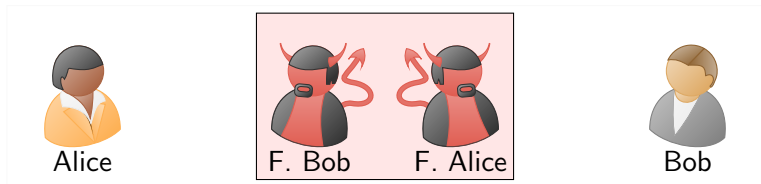


Bob

Attaques par relais

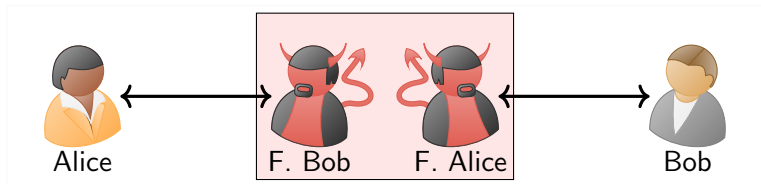


Attaques par relais



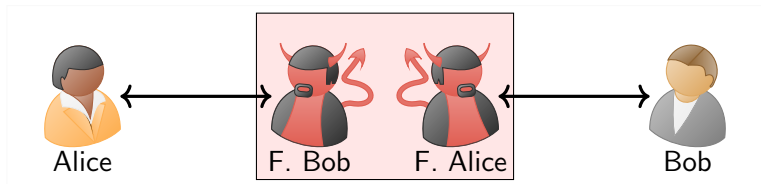
Principe : introduire un faux couple d'interlocuteurs entre deux correspondants légitimes.

Attaques par relais



Principe : introduire un faux couple d'interlocuteurs entre deux correspondants légitimes.

Attaques par relais



Principe : introduire un faux couple d'interlocuteurs entre deux correspondants légitimes.

Exemples d'attaques par relais :

- faux terminaux de paiement par cartes bancaires ;
- interception d'email ;
- systèmes de vote électronique ;
- communications radios ;
- etc.

Protection par utilisation d'un tiers de confiance

Organisme habilité qui va attester que l'interlocuteur contacté est légitime.



Alice



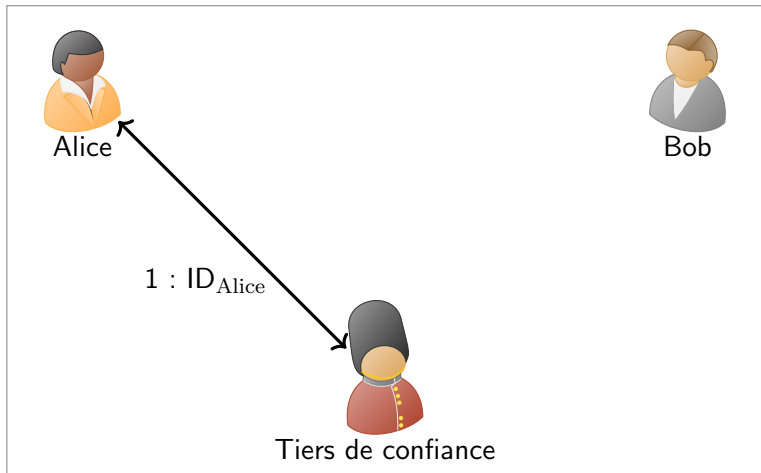
Bob



Tiers de confiance

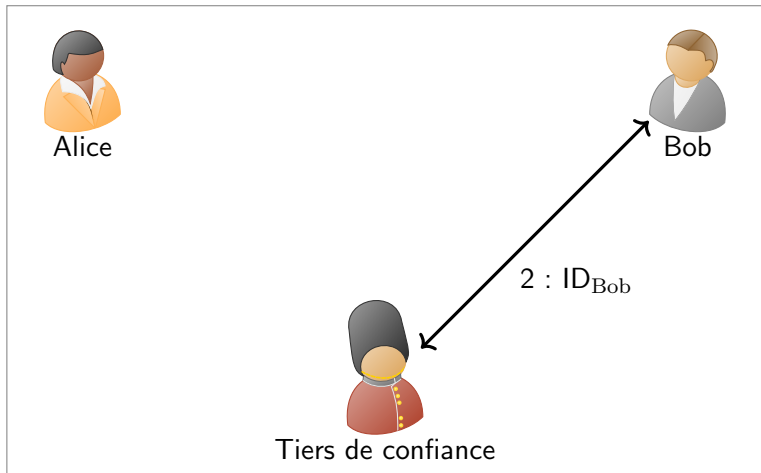
Protection par utilisation d'un tiers de confiance

Organisme habilité qui va attester que l'interlocuteur contacté est légitime.



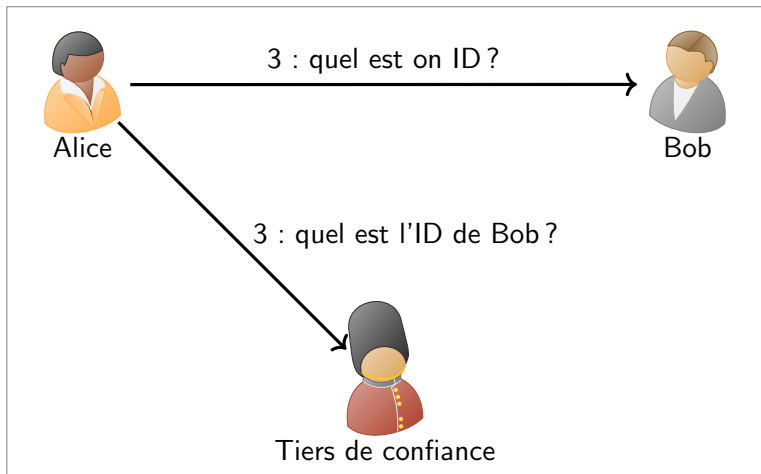
Protection par utilisation d'un tiers de confiance

Organisme habilité qui va attester que l'interlocuteur contacté est légitime.



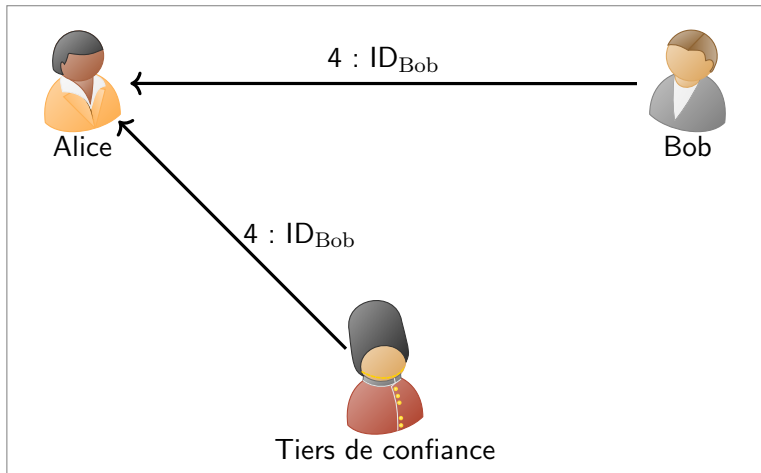
Protection par utilisation d'un tiers de confiance

Organisme habilité qui va attester que l'interlocuteur contacté est légitime.



Protection par utilisation d'un tiers de confiance

Organisme habilité qui va attester que l'interlocuteur contacté est légitime.



Protection par utilisation d'un tiers de confiance

Organisme habilité qui va attester que l'interlocuteur contacté est légitime.



Alice



Pirate, problème ID_{Bob} ???



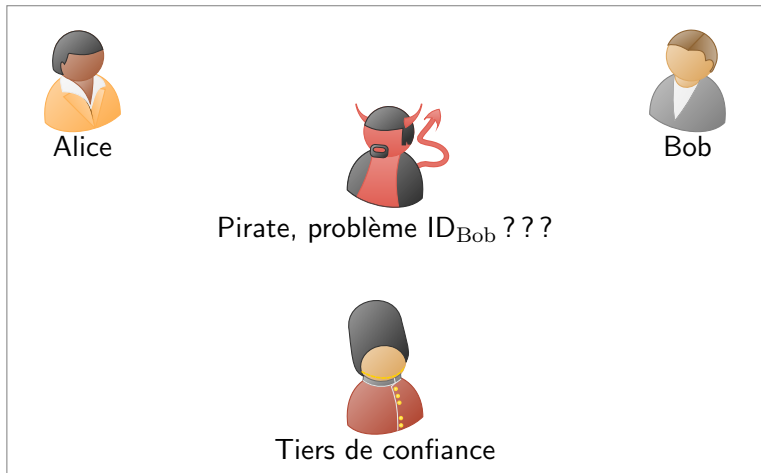
Bob



Tiers de confiance

Protection par utilisation d'un tiers de confiance

Organisme habilité qui va attester que l'interlocuteur contacté est légitime.



En pratique, c'est un peu plus compliqué car le tiers de confiance ne doit pas donner à Alice l'ID_{Bob} secret de Bob (on utilise des techniques plus complexes).

Exemple d'impact indirect des réseaux sociaux

Lors de la création d'un nouveau compte, on vous demande souvent de choisir un couple question/réponse pour retrouver votre mot de passe (c'est bien mais attention).

Exemple d'impact indirect des réseaux sociaux

Lors de la création d'un nouveau compte, on vous demande souvent de choisir un couple question/réponse pour retrouver votre mot de passe (c'est bien mais attention).

Est-ce bien raisonnable de choisir le « nom de jeune fille de votre mère » si ces informations sont disponibles à travers les réseaux sociaux ?

Probablement non, aujourd'hui Big Brother est partout et vous l'aidez !!!

Stockage de textes dans un ordinateur

Caractère = lettre d'un alphabet donné, p. ex. $\{A,B,\dots,Z,a,b,\dots,z\}$, stocké comme un nombre entier dans la mémoire de l'ordinateur, p. ex. $A=65$, $B=66$, $C=67$,

Chaîne de caractères = suite de caractères stockés l'un après l'autre en mémoire (on parle aussi de tableau de caractères).

Exemple : $M = \text{"FETE SCIENCE"}$

F	E	T	E		S	C	I	E	N	C	E
70	69	84	69	32	83	67	73	69	78	67	69
0	1	2	3	4	5	6	7	8	9	10	11

$M[0] = \text{'F'}$, $M[1] = \text{'E'}$, $M[2] = \text{'T'}$, ...

Comparaison de 2 caractères = faire la différence puis regarder le résultat.

Nombre de mots de passe possibles

Hypothèses :

- alphabet de ℓ lettres possibles ;
- mot de passe = chaîne de n caractères.

Nombre de mots de passe possibles $= \ell^n = \underbrace{\ell \times \ell \times \dots \times \ell}_{n \text{ fois}}$

Nombre de mots de passe possibles

Hypothèses :

- alphabet de ℓ lettres possibles ;
- mot de passe = chaîne de n caractères.

Nombre de mots de passe possibles $= \ell^n = \underbrace{\ell \times \ell \times \dots \times \ell}_{n \text{ fois}}$

Exemple 1 : $\{a,b\}$, $\ell = 2$, $n = 3$, on a $2^3 = 8$ mots de passe possibles :

aaa	aab	aba	abb	baa	bab	bba	bbb
-----	-----	-----	-----	-----	-----	-----	-----

Nombre de mots de passe possibles

Hypothèses :

- alphabet de ℓ lettres possibles ;
- mot de passe = chaîne de n caractères.

Nombre de mots de passe possibles = $\ell^n = \underbrace{\ell \times \ell \times \dots \times \ell}_{n \text{ fois}}$

Exemple 1 : $\{a,b\}$, $\ell = 2$, $n = 3$, on a $2^3 = 8$ mots de passe possibles :

aaa	aab	aba	abb	baa	bab	bba	bbb
-----	-----	-----	-----	-----	-----	-----	-----

Exemple 2 : $\{A,B,\dots,Z,a,b,\dots,z\}$, $\ell = 52$, $n = 8$:

$$52^8 = 53\,459\,728\,531\,456$$

Un programme de vérification de mot de passe

Entrées/sortie :

- entrée : M mot de passe donné par l'utilisateur (8 caractères)
- entrée : R mot de passe de référence, secret (8 caractères)
- sortie : valeur 1 = "autorisé" / valeur 0 = "pas autorisé"

Programme :

```
1  boucle: pour chaque position  $p$  entre 0 et 7 faire
2      |   si  $M[p] \neq R[p]$  alors sortir(0)
3  fin de boucle
4  sortir(1)
```

Un mauvais programme de vérification de mot de passe

Entrées/sortie :

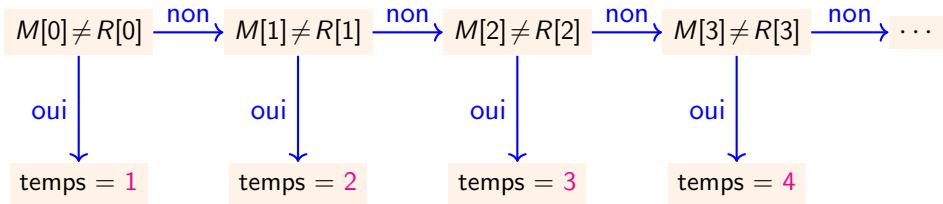
- entrée : M mot de passe donné par l'utilisateur (8 caractères)
- entrée : R mot de passe de référence, secret (8 caractères)
- sortie : valeur **1** = “autorisé” / valeur **0** = “pas autorisé”

Programme :

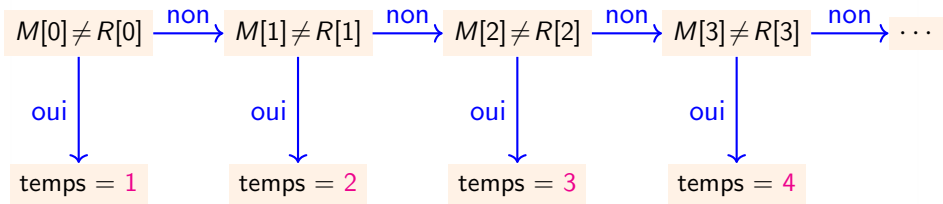
```
1  boucle: pour chaque position  $p$  entre 0 et 7 faire
2      |   si  $M[p] \neq R[p]$  alors sortir(0)
3  fin de boucle
4  sortir(1)
```

Vulnérabilité : variations du temps d'exécution en fonction du nombre de bons caractères durant l'exécution.

Analyse du temps de calcul du programme

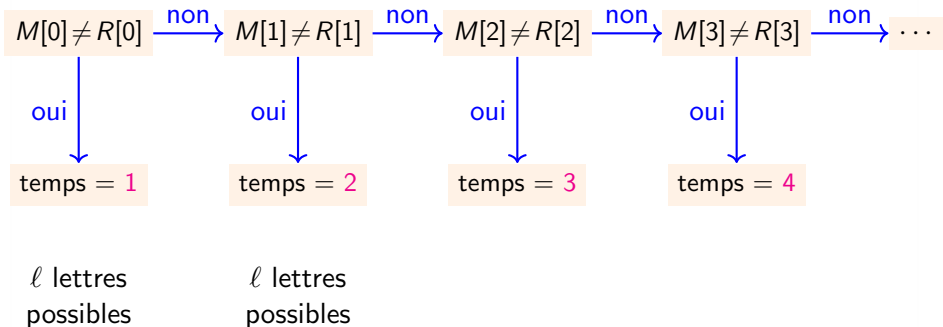


Analyse du temps de calcul du programme

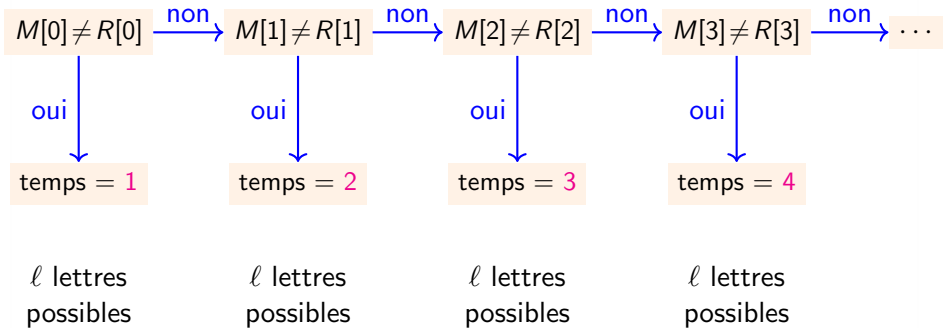


ℓ lettres
possibles

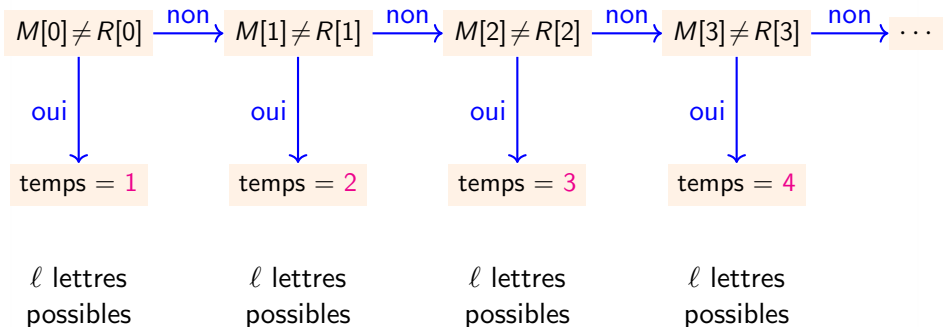
Analyse du temps de calcul du programme



Analyse du temps de calcul du programme

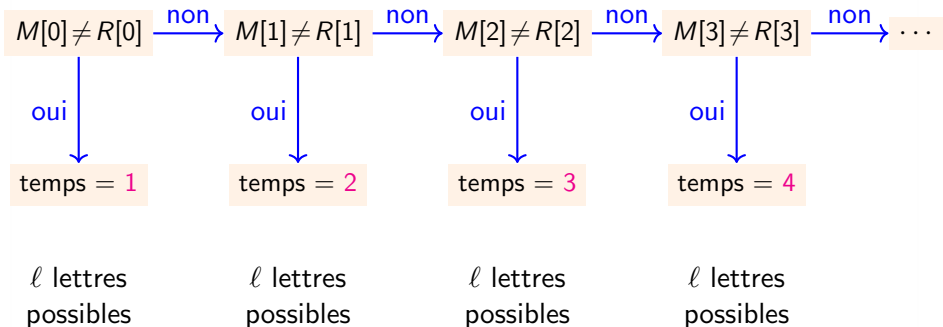


Analyse du temps de calcul du programme



Nombre total de tests à effectuer : $\underbrace{\ell + \ell + \dots + \ell}_{n \text{ fois}} = \ell \times n$.

Analyse du temps de calcul du programme



Nombre total de tests à effectuer : $\underbrace{\ell + \ell + \dots + \ell}_{n \text{ fois}} = \ell \times n.$

Pour $\ell = 52$ et $n = 8$:

$$\text{nb. tests attaque : } 52 \times 8 = 416$$

$$\text{nb. combinaisons : } 52^8 = 53\,459\,728\,531\,456$$

Protection contre cette attaque

Idée simple : avoir toujours le même temps de calcul.

Protection contre cette attaque

Idée simple : avoir toujours le même temps de calcul.

Nouveau programme :

```
1  x = 0
2  boucle: pour chaque position p entre 0 et 7 faire
3      |   si M[p] = R[p] alors x = x + 1
4      |                                   sinon x = x - 1
5  fin de boucle
6  si x = 8 alors sortir(1)
7      sinon sortir(0)
```

Protection contre cette attaque

Idée simple : avoir toujours le même temps de calcul.

Nouveau programme :

```
1  x = 0
2  boucle: pour chaque position p entre 0 et 7 faire
3      |   si M[p] = R[p] alors x = x + 1
4      |                                   sinon x = x - 1
5  fin de boucle
6  si x = 8 alors sortir(1)
7      sinon sortir(0)
```

Remarque : ce n'est **pas suffisant** (il existe d'autres types d'attaques). En pratique, il faut chiffrer (*crypter*) les mots de passe et utiliser des fonctions particulières sans jamais déchiffrer.

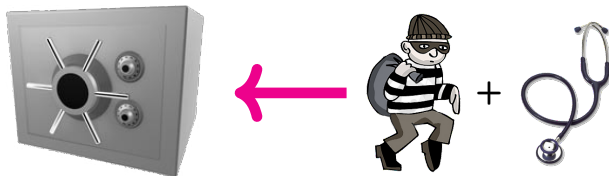
Attaques par canaux cachés, une nouvelle technique ?

Attaques par canaux cachés, une nouvelle technique ?

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

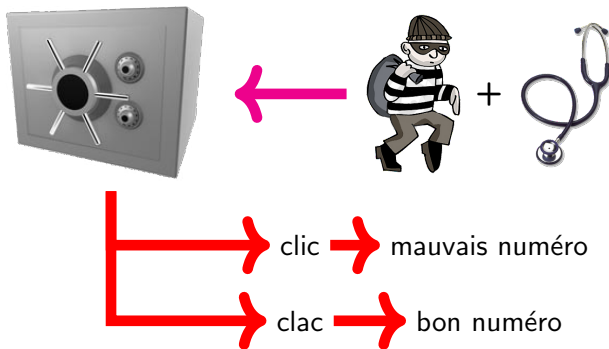
Attaques par canaux cachés, une nouvelle technique ?

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...



Quelles grandeurs physiques mesurer ?

Réponse : **tout** ce qui « entre » ou « sort » dans le ou du circuit

- temps de calcul
- consommation d'énergie
- rayonnement électromagnétique (REM)
- température
- bruit
- nombre de défauts de cache d'un ordinateur
- nombre et type des messages d'erreur
- ...

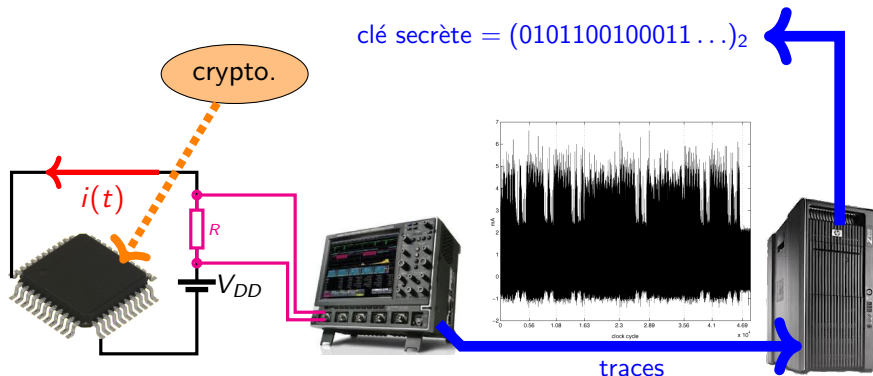
Les valeurs mesurées peuvent révéler des informations sur :

- le comportement **global** (conso., REM, température, bruit ...)
- le comportement **local** (REM local, nb. déf. cache ...)

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

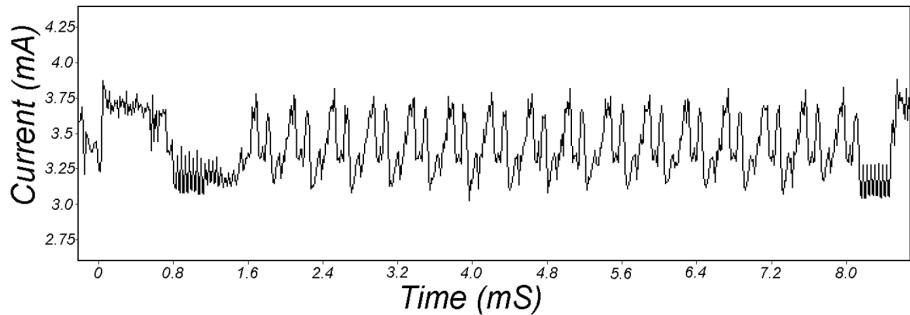


V_{DD} est la tension d'alimentation du circuit

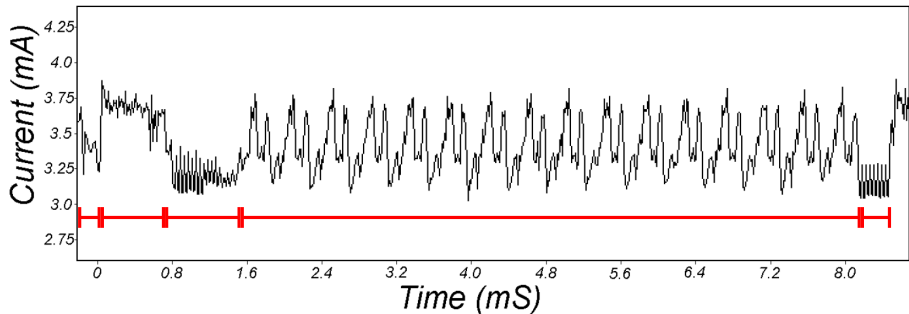
Banc d'attaque par analyse de consommation



Que « lire » dans les traces ?

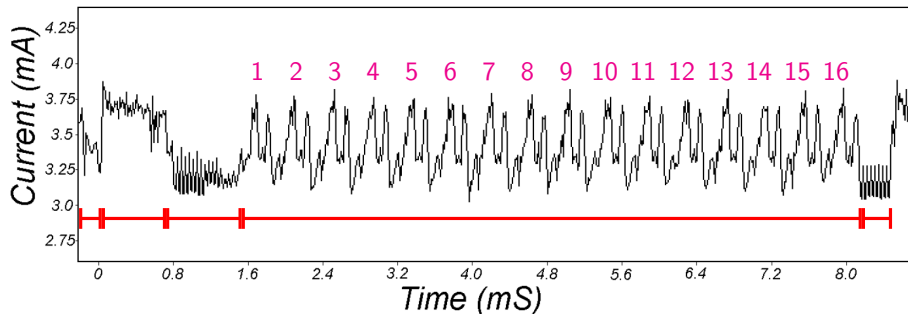


Que « lire » dans les traces ?



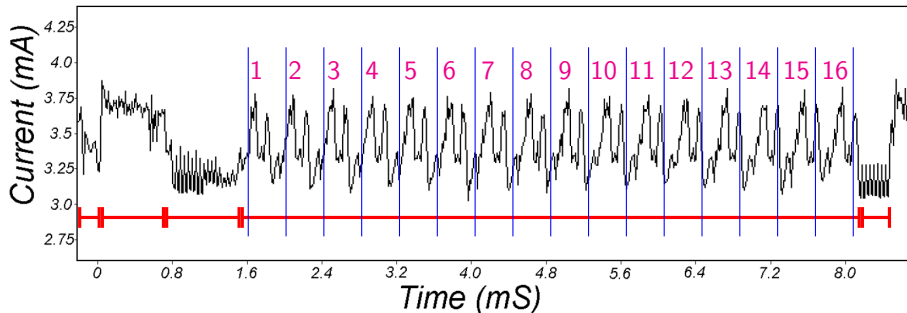
- algorithme $\Rightarrow$ découpage en étapes

Que « lire » dans les traces ?



- algorithme $\Rightarrow$ découpage en étapes
- détection des tours de boucle (calculs répétitifs)
 - ▶ temps constant dans un tour

Que « lire » dans les traces ?



- algorithme $\Rightarrow$ découpage en étapes
- détection des tours de boucle (calculs répétitifs)
 - ▶ temps constant dans un tour
 - ▶ ou pas ???

Exploiter les différences

Un algorithme a une **signature** :

```
 $r = c_0$   
for  $i$  from 1 to  $n$  do  
  if  $a_i = 0$  then  
     $r = r + c_1$   
  else  
     $r = r \times c_2$ 
```

Exploiter les différences

Un algorithme a une **signature** en **courant** :

```
 $r = c_0$   
for  $i$  from 1 to  $n$  do  
  if  $a_i = 0$  then  
     $r = r + c_1$   
  else  
     $r = r \times c_2$ 
```

I_+ $I_\times$

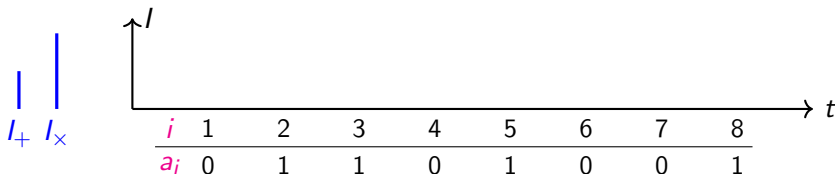
Exploiter les différences

Un algorithme a une **signature** en **courant** :

```

r = c0
for i from 1 to n do
    if ai = 0 then
        r = r + c1
    else
        r = r × c2

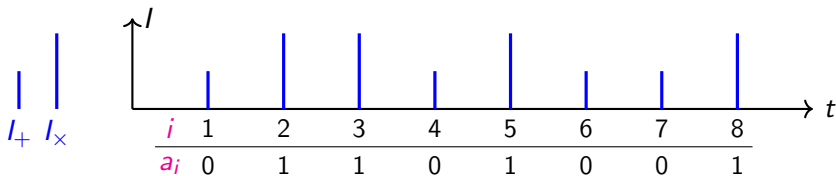
```



Exploiter les différences

Un algorithme a une **signature** en **courant** :

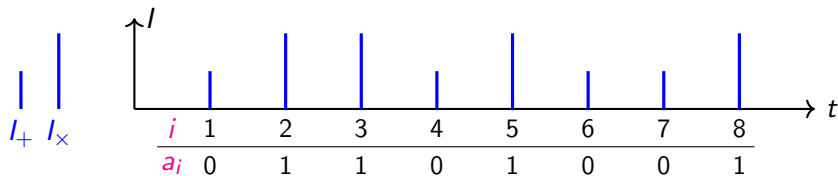
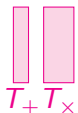
```
 $r = c_0$   
for  $i$  from 1 to  $n$  do  
  if  $a_i = 0$  then  
     $r = r + c_1$   
  else  
     $r = r \times c_2$ 
```



Exploiter les différences

Un algorithme a une **signature** en **courant** et en **temps de calcul** :

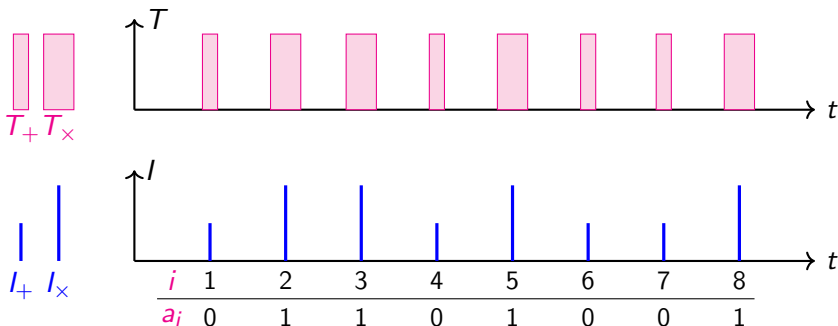
```
 $r = c_0$   
for  $i$  from 1 to  $n$  do  
  if  $a_i = 0$  then  
     $r = r + c_1$   
  else  
     $r = r \times c_2$ 
```



Exploiter les différences

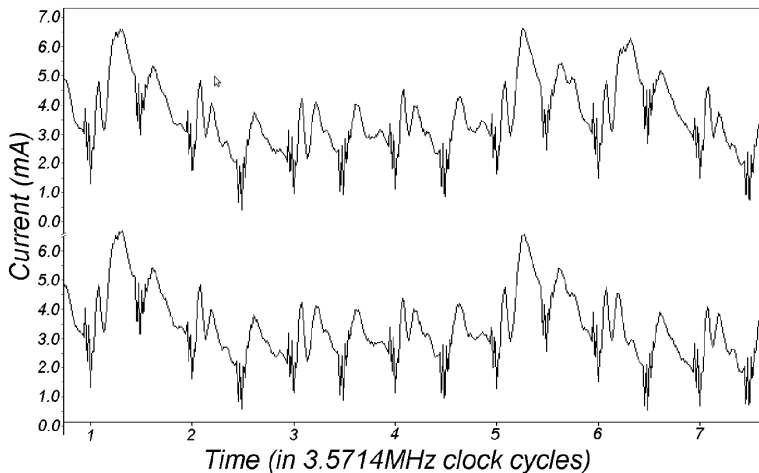
Un algorithme a une **signature** en **courant** et en **temps de calcul** :

```
 $r = c_0$   
for  $i$  from 1 to  $n$  do  
  if  $a_i = 0$  then  
     $r = r + c_1$   
  else  
     $r = r \times c_2$ 
```



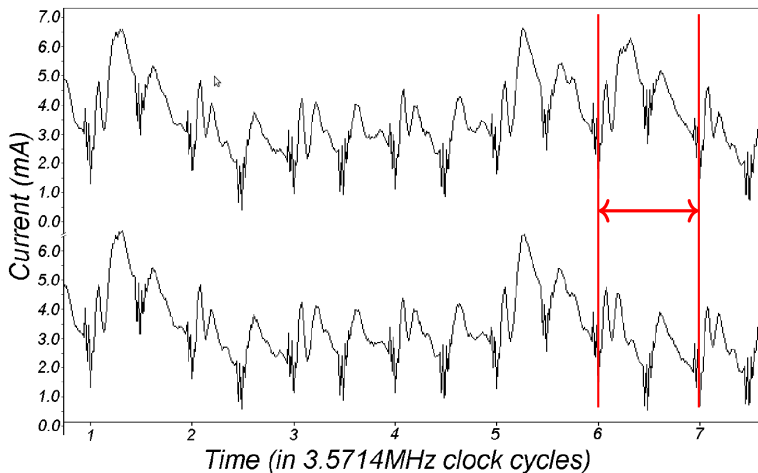
Analyse simple de la consommation (SPA)

En anglais : SPA *simple power analysis*



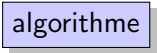
Analyse simple de la consommation (SPA)

En anglais : SPA *simple power analysis*



La SPA en pratique

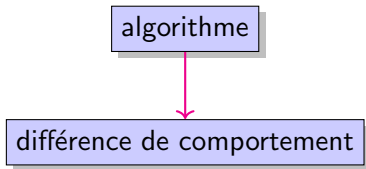
Principe :



algorithme

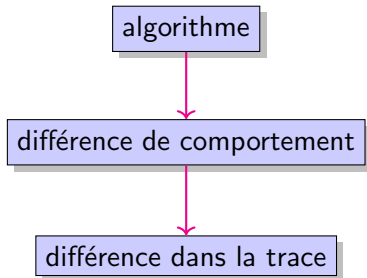
La SPA en pratique

Principe :



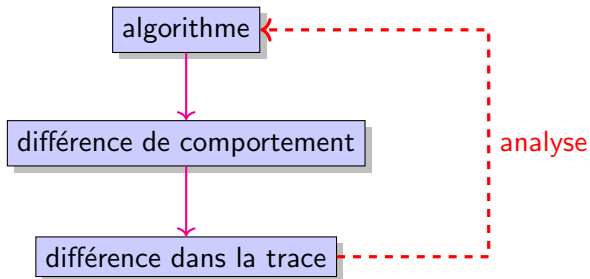
La SPA en pratique

Principe :



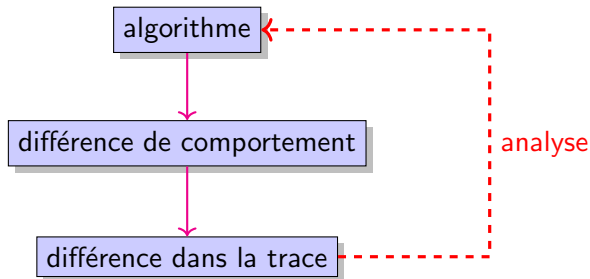
La SPA en pratique

Principe :



La SPA en pratique

Principe :

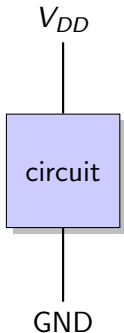


Techniques : exploiter les différences dans

- le contrôle
- le temps de calcul
- les valeurs des opérandes (temps de calcul, conso., REM...)
- ...

Attaque par analyse du REM

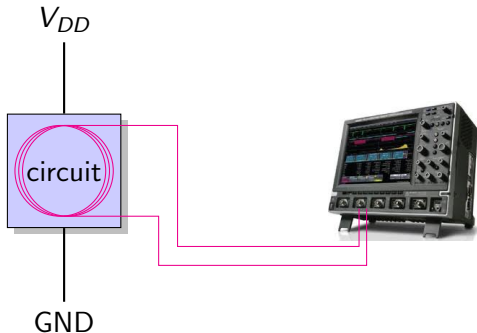
Principe général : utiliser une sonde pour mesurer le REM



Mesures du REM :

Attaque par analyse du REM

Principe général : utiliser une sonde pour mesurer le REM

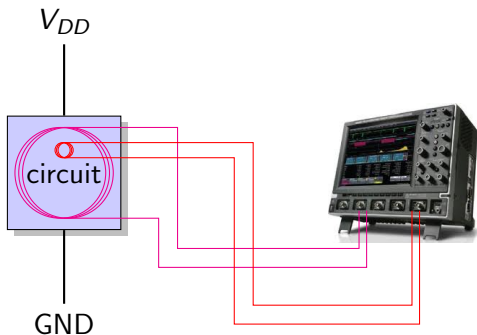


Mesures du REM :

- global avec une sonde large

Attaque par analyse du REM

Principe général : utiliser une sonde pour mesurer le REM

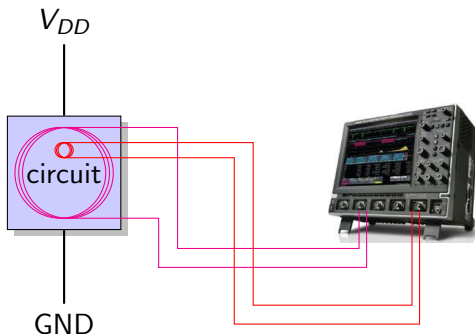


Mesures du REM :

- global avec une sonde large
- local avec une micro-sonde

Attaque par analyse du REM

Principe général : utiliser une sonde pour mesurer le REM



Mesures du REM :

- global avec une sonde large
- local avec une micro-sonde
- cartographie fine du circuit avec une table XY

Principales techniques de protection

Empêcher une (ou des) attaques par :

- un nouveau dispositif de protection
- la modification/sécurisation du dispositif original

Principales techniques de protection

Empêcher une (ou des) attaques par :

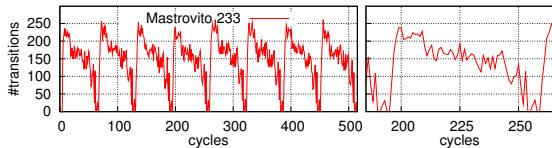
- un nouveau dispositif de protection
- la modification/**sécurisation** du dispositif original

Exemples :

- blindage
- uniformiser les temps de calcul
- uniformiser la consommation d'énergie
- utiliser des codes détecteurs/correcteurs d'erreurs
- introduire du bruit (instructions inutiles)
- reconfigurer le circuit
 - ▶ changer le codage des données
 - ▶ changer les algorithmes

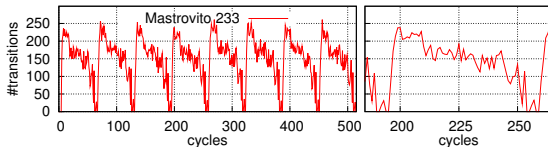
Contre-mesure : opérateurs arithmétiques sécurisés

Multiplier non protégé

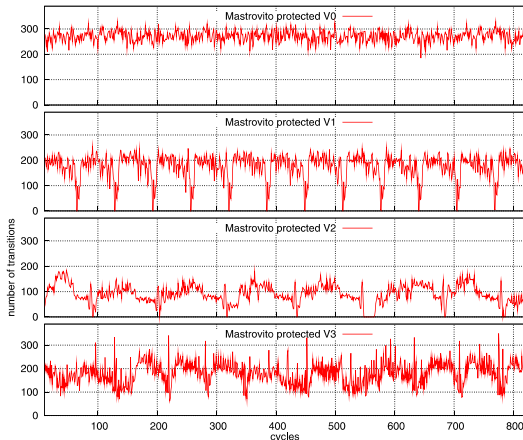


Contre-mesure : opérateurs arithmétiques sécurisés

Multiplier non protégé



Multiplieurs protégés



Agence nationale de la sécurité des systèmes d'information

ANSSI : <https://www.ssi.gouv.fr/>

Aspects réglementaires, certifications, recommandations et excellente source d'informations très accessibles pour les administrations, entreprises et particuliers.

Exemples de documents très intéressants :

- guide des bonnes pratiques de l'informatique ;
- partir en mission avec son téléphone, sa tablette ou son ordinateur portable ;
- sécuriser un site web ;
- sécuriser les accès Wi-Fi ;
- guide d'hygiène informatique ;
- sécurité des mots de passe ;
- etc.

Conclusion (très partielle)

- Attaques de plus en plus performantes

Conclusion (très partielle)

- **Attaques** de plus en plus **performantes**
- Sécurisation nécessaire à **tous les niveaux** (théorie, algorithmes, opérations, implantations, formation des utilisateurs, . . .)

Conclusion (très partielle)

- **Attaques** de plus en plus **performantes**
- Sécurisation nécessaire à **tous les niveaux** (théorie, algorithmes, opérations, implantations, formation des utilisateurs, . . .)
- Sécurisation = compromis entre utilisabilité et robustesse

Conclusion (très partielle)

- **Attaques** de plus en plus **performantes**
- Sécurisation nécessaire à **tous les niveaux** (théorie, algorithmes, opérations, implantations, formation des utilisateurs, ...)
- Sécurisation = compromis entre utilisabilité et robustesse
- Coût de sécurisation = *fonction*(valeur secret, type attaquant)

Conclusion (très partielle)

- **Attaques** de plus en plus **performantes**
- Sécurisation nécessaire à **tous les niveaux** (théorie, algorithmes, opérations, implantations, formation des utilisateurs, ...)
- Sécurisation = compromis entre utilisabilité et robustesse
- Coût de sécurisation = *fonction*(valeur secret, type attaquant)
- **Sécurité** = mathématiques + informatique + micro-électronique + droit + sciences sociales + ...

Conclusion (très partielle)

- **Attaques** de plus en plus **performantes**
- Sécurisation nécessaire à **tous les niveaux** (théorie, algorithmes, opérations, implantations, formation des utilisateurs, ...)
- Sécurisation = compromis entre utilisabilité et robustesse
- Coût de sécurisation = *fonction*(valeur secret, type attaquant)
- **Sécurité** = mathématiques + informatique + micro-électronique + droit + sciences sociales + ...

On estime qu'il faut environ **10 000 ingénieurs et techniciens** formés dans les métiers de la cybersécurité en France pour les prochaines années !

La Bretagne est un acteur majeur du domaine avec le **Pôle d'Excellence Cyber** (PEC) aux niveaux industriel, recherche et formation.

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