Journée Science Ouverte

8 octobre 2020

Provable Mitigation of Side Channel through Parametric Verification

Étienne André[1], Sudipta Chattopadhyay[2], Didier Lime[3], Olivier H. Roux[3], and Sun Jun[4]

[1] Université de Lorraine, CNRS, Inria, LORIA, Nancy, France
[2] Singapore University of Technology and Design
[3] LS2N, École Centrale Nantes, France
[4] Singapore Management University

Projet ANR (France) – NRF (Singapour) 2020–2023

	Étienne André	Université de Lorraine, France
	Sudipta Chattopadhyay	SUTD
	Didier Lime	École Centrale Nantes, France
	Olivier H. Roux	École Centrale Nantes, France
	Jun Sun	Singapore Management University

Contexte : attaques par canaux auxiliaires

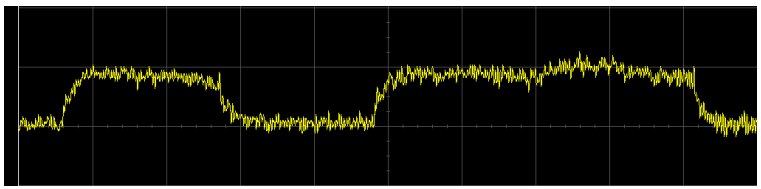
- Exemple
  - Nombre de pizzas commandées par la Maison blanche la veille d'annonces d'entrée en guerre des USA [1]

1. `http://home.xnet.com/~warinner/pizzacites.html`

Contexte : attaques par canaux auxiliaires

- Exemple
  - Nombre de pizzas commandées par la Maison blanche la veille d'annonces d'entrée en guerre des USA [1]

- Menaces sur un système informatique
  - Attaques par observation de la consommation d'électricité



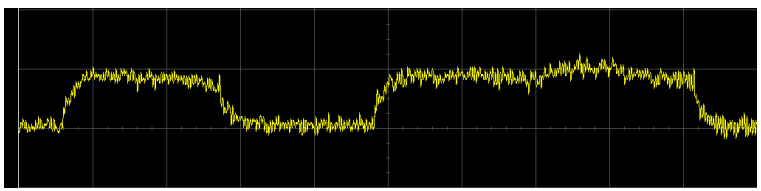
  - Attaques par rayonnement électromagnétique
  - Attaques par cache
  - Attaques acoustiques
  - Attaques temporisées
  - etc.

1. `http://home.xnet.com/~warinner/pizzacites.html`

Contexte : attaques par canaux auxiliaires

- Exemple
  - Nombre de pizzas commandées par la Maison blanche la veille d'annonces d'entrée en guerre des USA [1]

- Menaces sur un système informatique
  - Attaques par observation de la consommation d'électricité



  - Attaques par rayonnement électromagnétique
  - Attaques par cache
  - Attaques acoustiques
  - Attaques temporisées
  - etc.

1. `http://home.xnet.com/~warinner/pizzacites.html`

Exemple d'attaque temporisée

```
1 # input pwd    : Real password
2 # input attempt: Tentative password
3 for i = 0 to min(len(pwd, len(attempt)) - 1 do
4     if pwd[i] =/= attempt[i] then
5     return false
6 done
7 return true
```

Exemple d'attaque temporisée

```
1 # input pwd    : Real password
2 # input attempt: Tentative password
3 for i = 0 to min(len(pwd, len(attempt)) - 1 do
4     if pwd[i] =/= attempt[i] then
5     return false
6 done
7 return true
```

pwd	c	h	o	r	i	z	o
attempt	c	h	e	e	s	e	

Temps d'exécution :

Exemple d'attaque temporisée

```
1 # input pwd    : Real password
2 # input attempt: Tentative password
3 for i = 0 to min(len(pwd, len(attempt)) - 1 do
4     if pwd[i] =/= attempt[i] then
5     return false
6 done
7 return true
```

pwd	c	h	o	r	i	z	o
attempt	c	h	e	e	s	e	

Temps d'exécution : ϵ

Exemple d'attaque temporisée

```
1 # input pwd    : Real password
2 # input attempt: Tentative password
3 for i = 0 to min(len(pwd, len(attempt)) - 1 do
4     if pwd[i] =/= attempt[i] then
5     return false
6 done
7 return true
```

pwd	c	h	o	r	i	z	o
attempt	c	h	e	e	s	e	

Temps d'exécution : $\epsilon + \epsilon$

Exemple d'attaque temporisée

```
1 # input pwd    : Real password
2 # input attempt: Tentative password
3 for i = 0 to min(len(pwd, len(attempt)) - 1 do
4     if pwd[i] =/= attempt[i] then
5     return false
6 done
7 return true
```

pwd	c	h	o	r	i	z	o
attempt	c	h	e	e	s	e	

Temps d'exécution : $\epsilon + \epsilon + \epsilon$

Exemple d'attaque temporisée

```
1 # input pwd    : Real password
2 # input attempt: Tentative password
3 for i = 0 to min(len(pwd, len(attempt)) - 1 do
4     if pwd[i] =/= attempt[i] then
5     return false
6 done
7 return true
```

pwd	c	h	o	r	i	z	o
attempt	c	h	e	e	s	e	

Temps d'exécution : $\epsilon + \epsilon + \epsilon$

- Problème : le temps d'exécution est proportionnel au nombre de caractères consécutifs corrects à partir du début de `attempt`

Objectifs du projet

Objectif de ProMiS

Détecter et mitiger des attaques par canal temporisé sur des programmes informatiques à l'aide de méthodes formelles

`https://www.loria.science/ProMiS/`

Contenu de notre plan de gestion des données

Contenu :

- Programmes informatiques que nous allons étudier
  - « Bibliothèques d'études de cas » (*benchmarks*)
    - Ici : majoritairement des programmes informatiques
  - Études de cas existantes, ou nouvelles

- Métadonnées : essentiellement source de ces études de cas, vulnérabilité…

Diffusion :

- Diffusion publique (Web)
- Licence libre (par exemple GNU-GPL) permettant leur réutilisation

Difficultés

Globalement peu de difficultés à rédiger le plan

Raisons :

- Données de taille raisonnablement modeste
  - Quelques dizaines d'études de cas de quelques centaines de lignes de code
- Pas de données personnelles ou sensibles
- L'intégralité de ces données peut être conservée longtemps
  - Question ouverte : entrepôts institutionnels, ou type Zenodo

Retour d'expérience

Yet another tâche administrative rébarbative ?

- Oui : un formulaire de plus à remplir
- Non : plein de questions utiles à se poser (conservation, réutilisation, partage…)

Aide bienvenue de l'Université de Lorraine

- ☺ Merci à Laetitia Bracco

Réflexion à plus long terme :

- Systématisation de l'ouverture et la conservation des données dans les domaines qui peuvent se le permettre ?

Licensing

Source of the graphics used I

Title : Power attack
Author : Audriusa
Source : `https://commons.wikimedia.org/wiki/File:Power_attack.png`
License : GNU GPL

License of this document

Author : **Étienne André**