RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Inria

cea

université de BORDEAUX

Analyse automatisée d'une bibliothèque crypographique

Détection de failles par canal auxiliaire par analyse statique et symbolique

Duzés Florian

Master Cryptologie et Sécurité Informatique

28 août 2025

Opérations dangereuses

Opérations influantes :

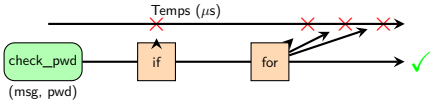
- Accès mémoire
- Décalage/rotation de valeurs
- Saut conditionnel
- Division/multiplication

Opérations dangereuses

Opérations influantes :

- Accès mémoire
- Décalage/rotation de valeurs (caché)
- Saut conditionnel
- Division/multiplication

```
1   bool check_pwd(msg, pwd){
2   if (msg.length != pwd.length){
3       return False
4   }
5   for(int i = 0; i < msg.length; i++){
6       if(msg[i] != pwd[i]){
7           return False
8       }
9   }
10  return True
11  }
```



Plus de problème ?

Plus de problème ?

Mauvaises nouvelles ?

2019 : Daniel, Bardin et Rezk, *Binsec/Rel : Efficient Relational Symbolic Execution for Constant-Time at Binary-Level*

Plus de problème ?

Mauvaises nouvelles !

2019 : Daniel, Bardin et Rezk, *Binsec/Rel : Efficient Relational Symbolic Execution for Constant-Time at Binary-Level*
2024 : Schneider et al., *Breaking Bad : How Compilers Break Constant-Time Implementations*

Spécialisations

Outil	Cible	Techn.	Garanties
ctgrind [Lan10]	Binaire	Dynamique	▲
ABPV13 [Alm+13]	C	Formel	●
VirtualCert [Bar+14]	x86	Formel	●
ct-verif [Bar+16]	LLVM	Formel	●
FlowTracker [RPA16]	LLVM	Formel	●
Blazer [Ant+17]	Java	Formel	●
BPT17 [BPT17]	C	Symbolique	▲
MemSan [Tea17]	LLVM	Dynamique	▲
Themis [CFD17]	Java	Formel	●
COCO-CHANNEL [Bre+18]	Java	Symbolique	●
DATA [Wei+20] ; [Wei+18]	Binaire	Dynamique	▲
MicroWalk [Wic+18]	Binaire	Dynamique	▲
timecop [Nei18]	Binaire	Dynamique	▲
SC-Eliminator [Wu+18]	LLVM	Formel	●
Binsec/Rel [DBR19]	Binaire	Symbolique	▲
CT-WASM [Wat+19]	WASM	Formel	●
FaCT [Cau+19]	DSL	Formel	●
haybale-pitchfork [Dis20]	LLVM	Symbolique	▲

Liste d'outils de vérification

Source : [Jan+21]

Cible

- [C, Java] Code source
- Binaire Binaire
- DSL Surcouche de langage
- Trace Trace d'exécution
- WASM Assembleur web

Techn.

- Formel Programmation formelle
- [*] type d'analyse

Garanties (attaques temporelles)

● = Analyse correcte, ▲ = Limitée

empty

empty

empty