Plateforme de protection de binaires configurable et dynamiquement adaptative

Kévin Le Bon

Dirigé par : Erven Rohou
Encadré par : Frédéric Tronel et Guillaume Hiet

Inria Rennes-Bretagne Atlantique

RESSI
15 mai 2019

Corruption de la mémoire : définition et objectifs

Corruption de mémoire

Une attaque par corruption de mémoire consiste en la modification de la mémoire du processus cible afin d'en altérer le comportement.

Les possibilités sont variées :

- Faire fuiter des informations
- Modifier des données manipulées par le programme
- Faire exécuter du code arbitraire par la machine

Corruption de la mémoire : une menace toujours d'actualité

Articles traitant des corruptions de mémoire

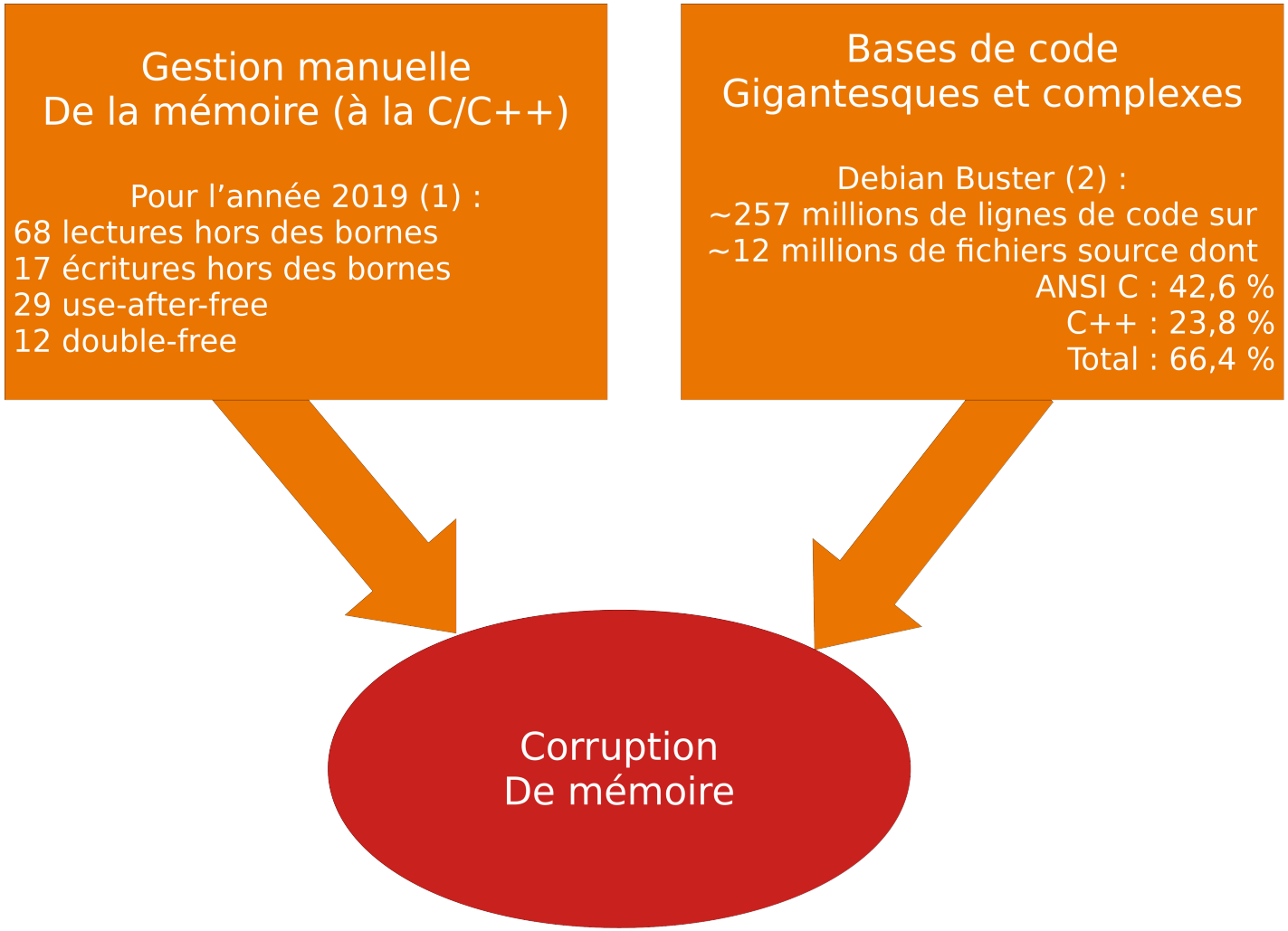
- "Smashing the stack for fun and profit", Phrack 1996
- "A compile-time solution to buffer overflow attacks", ICDCS 2001

Toujours une menace sérieuse

Programme	2017	2018	2019	Total
Chrome	45	50	19	114
Firefox	2	111	21	134

https://www.cvedetails.com/

Corruption de la mémoire : les causes



1: https://www.cvedetails.com/cwe-definitions.php
2: https://sources.debian.org/stats/

Surcoût en performances des solutions dynamiques

- De nombreuses politiques de sécurité permettent de s'en prémunir
- Certaines sont intégrées par défaut
  - Code integrity
  - Address-Space Randomization
  - Non-Executable Data
- D'autres sont trop coûteuses

Politique [1]	Solution	Surcoût en performances
Memory Safety	Softbound+CETS	116%
	AddressSanitizer	73%
CFI	Abadi	15% (max 45%)

Les protections sont actives pour l'ensemble du programme et durant toute l'exécution du processus

[1] Szekeres, Laszlo, et al. "Sok: Eternal war in memory." 2013 IEEE Symposium on Security and Privacy. IEEE, 2013.

Notre approche

Notre objectif

Réduire l'impact de telles protections sur les performances du processus cible

Pour ce faire

- Utilisation de la modification dynamique de binaire
  $\Rightarrow$ injecter des protections pendant l'exécution
- Analyses en parallèle du code et de l'état du processus

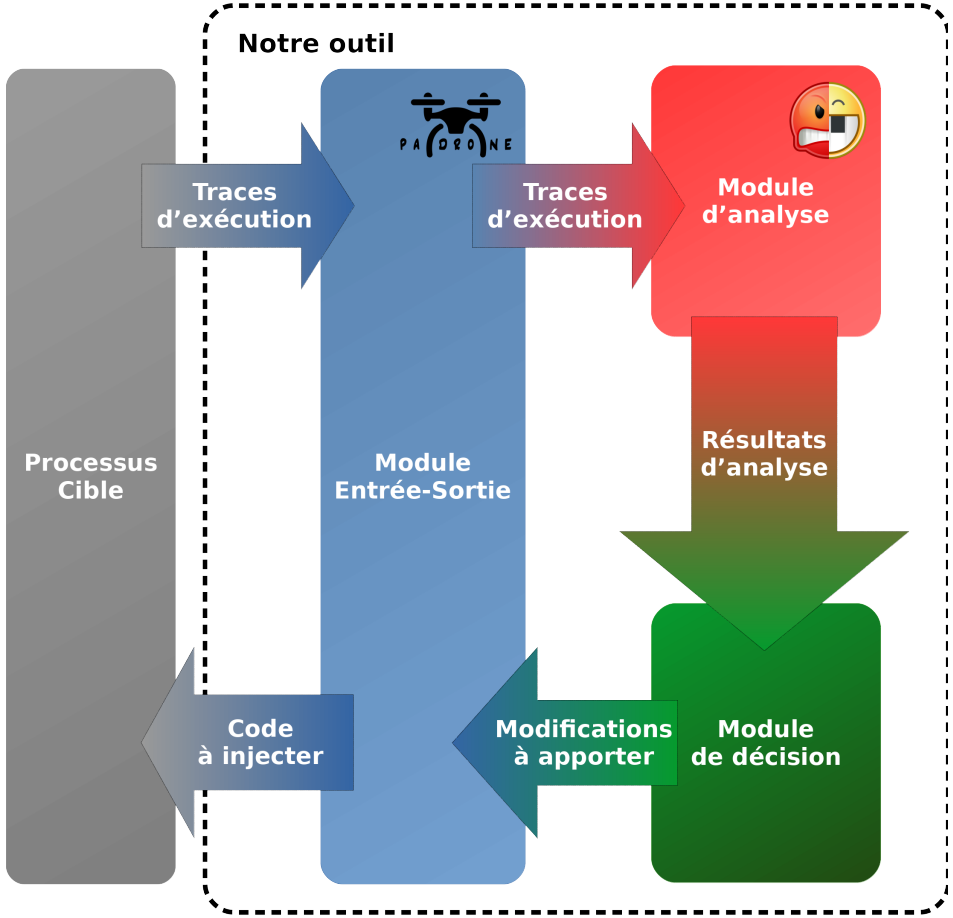
Idée centrale

Ne déployer des protections que lorsqu'elles sont utiles.

Principes

Un système dynamique basée sur trois fonctions :

- Calculer un niveau de menace
  - Analyse de l'état du processus
- Choisir la protection à déployer
  - La protection la plus pertinente selon le contexte
- Modifier le code du processus
  - Modification dynamique de binaire (DBM)



Merci de votre attention