PSL

CRGN
CENTRE DE RECHERCHE
GENDARMERIE NATIONALE

COMCYBER-MI

« Nos forces, pour votre cyber-protection »

L'injection de fautes comme outil d'investigation numérique

JAIF 2024

Nicolas HUGGET

1er Octobre 2024

Sommaire

Présentation de l'intervenant

Contexte

- **Études** :
  - Diplôme d'ingénieur
  - Mastère Sécurité publique
  - Mastère spécialisé IoT
- **Carrière** :
  - Ingénieur embarqué
  - Officier criminalistique
  - Apprentissage en sécurité matérielle
  - Chef de Laboratoire

Doctorant, équipe sécurité DI-ENS

Définition : *La criminalistique numérique vue par Interpol [1]*

La criminalistique numérique est une branche des sciences criminalistiques qui porte sur la recherche, l'acquisition, le traitement et l'analyse de données stockées sous forme numérique et sur la communication d'informations les concernant.

Définition : *La criminalistique numérique vue par Interpol [1]*

La criminalistique numérique est une branche des sciences criminalistiques qui porte sur la recherche, l'acquisition, le traitement et l'analyse de données stockées sous forme numérique et sur la communication d'informations les concernant.

Objectifs :

- Extraire les données des éléments de preuves numériques
- Les transformer en renseignements exploitables
- Mettre en forme ces renseignements pour les présenter devant un tribunal

Définition : *La criminalistique numérique vue par Interpol [1]*

La criminalistique numérique est une branche des sciences criminalistiques qui porte sur la recherche, l'acquisition, le traitement et l'analyse de données stockées sous forme numérique et sur la communication d'informations les concernant.

Objectifs :

- **Extraire les données des éléments de preuves numériques**
- Les transformer en renseignements exploitables
- Mettre en forme ces renseignements pour les présenter devant un tribunal

Les supports d'analyse

Contexte

Justice

Enquêteur

Justice

Enquêteur

Sommaire

Des contraintes pratiques

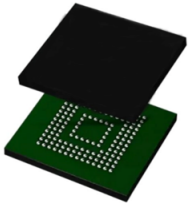
- ☞ Répétabilité du processus d'extraction.
- ☞ Coûts de l'extraction.
- ☞ Durée de l'extraction.

Des contraintes légale

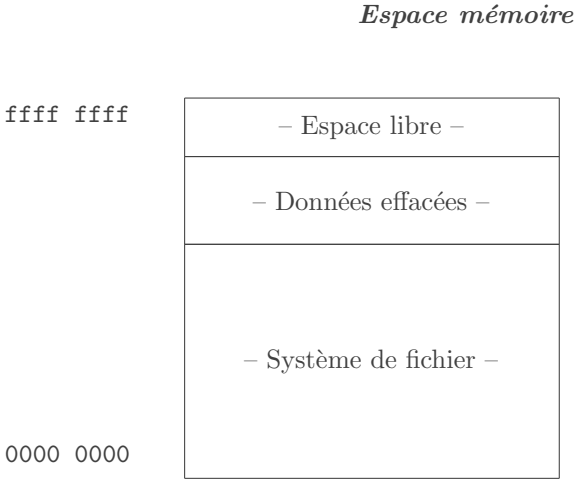
- ☞ Préservation de l'intégrité des données et du support.
- ☞ Légitimité de la preuve.

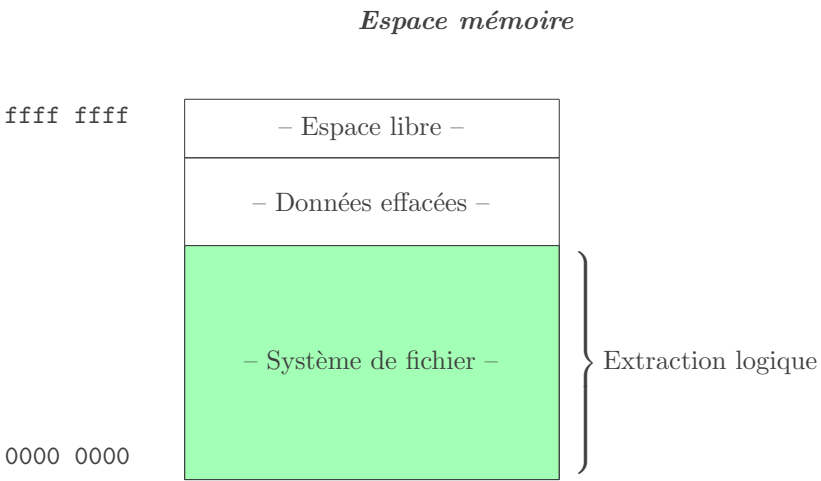
Disque dur plateau

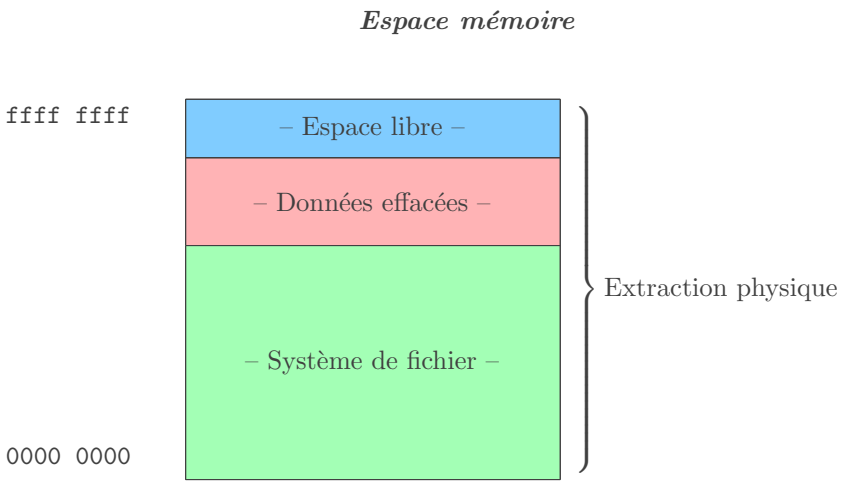
Mémoires Flash Brutes



Mémoires Flash Gérées


Espace mémoire
ffff ffff
– Espace libre –
– Données effacées –
– Système de fichier –
0000 0000


Espace mémoire
ffff ffff
– Espace libre –
– Données effacées –
– Système de fichier –
Extraction logique
0000 0000


Espace mémoire
ffff ffff
– Espace libre –
– Données effacées –
– Système de fichier –
0000 0000
Extraction physique

Pour sécurisé les données contenues dans les systèmes, les industriels ont mis en place des mécanismes de sécurité :

Légende : Présent ✓ Absent ✗

Mécanisme de protection	**Type d'extraction**	
	Logique	Physique
Verrouillage par mot de passe	✓	✓
Chiffrement des données	✓	✓
Mémoire non adressable	✓	✓
Chaîne de démarrage sécurisée	✓	✗

Sommaire

L'injection de fautes, un outil d'extraction ?

Définition : *Faute*

Effet obtenu suite à un dysfonctionnement dans un système.

L'injection de fautes, un outil d'extraction ?

Définition : *Faute*

Effet obtenu suite à un dysfonctionnement dans un système.

Définition : *Attaque par injection de faute*

Attaque visant a injecter une perturbation afin de créer le dysfonctionnement contrôler d'un système.

L'injection de fautes, un outil d'extraction ?

Définition : *Faute*

Effet obtenu suite à un dysfonctionnement dans un système.

Définition : *Attaque par injection de faute*

Attaque visant a injecter une perturbation afin de créer le dysfonctionnement contrôler d'un système.

- Attaques actives
- Perturbation de la tension d'alimentation, injection EM, utilisation de lumière concentrée
- Peuvent modifier le flot d'exécution d'un programme embarqué
- Peuvent permettre la fuite de clés d'algorithmes cryptographiques

Type de programme : Horizon 2020

Durée : 36 mois

Date de démarrage : 01/07/2020

Programme de collaboration européenne entre des entreprises et les forces de l'ordre pour mettre en place de nouvelles méthode d'extraction de données sur téléphones chiffrés.

Type de programme : Horizon 2020

Durée : 36 mois

Date de démarrage : 01/07/2020

Programme de collaboration européenne entre des entreprises et les forces de l'ordre pour mettre en place de nouvelles méthode d'extraction de données sur téléphones chiffrés.

☞ **Premier programme à se concentrer à la fois sur les volets matériels et logiciels.**

A new model for forensic data extraction from encrypted mobile devices, *Forensic Science International : Digital Investigation 2021*,

Aya Fukami et al. [4]

A new model for forensic data extraction from encrypted mobile devices, *Forensic Science International : Digital Investigation 2021*,

Aya Fukami et al. [4]

☞ Les attaques matérielles sont envisagées comme méthodes d'extraction de données sur des smartphones.

☞ Aborde l'aspect légal de la problématique sur le plan européen

Physical fault injection and side-channel attacks on mobile devices, *Computers & Security 2021*,

Shepherd Carlton et al. [5]

Physical fault injection and side-channel attacks on mobile devices, *Computers & Security 2021*,

Shepherd Carlton et al. [5]

- ☞ Fournis un état de l'art de plus de 50 attaques par canaux auxiliaires et injection de fautes
- ☞ Classe les attaques par niveau d'invasivité et d'altération

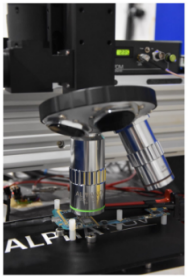
Laser-Induced Fault Injection on Smartphone Bypassing the Secure Boot, *Fault Diagnosis and Tolerance in Cryptography (FDTC) 2017*,
Vasselle Aurélien et al. [6]

Des réussites techniques

L'injection de fautes, un outil d'extraction ?

Laser-Induced Fault Injection on Smartphone Bypassing the Secure Boot, *Fault Diagnosis and Tolerance in Cryptography (FDTC) 2017*,
Vasselle Aurélien et al. [6]

- ☞ **LFI** applicable à un Soc de smartphone
- ✗ Matériel onéreux
- ✗ Énorme travail préparatoire



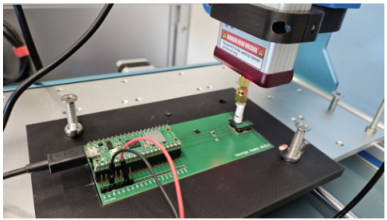
Keyless Entry : Breaking and Entering eMMC RPMB with EMFI.,
ACM Conference on Security and Privacy in Wireless and Mobile Networks. 2024,
Aya Fukami et al. [3]

Keyless Entry : Breaking and Entering eMMC RPMB with EMFI.,
ACM Conference on Security and Privacy in Wireless and Mobile Networks. 2024,
Aya Fukami et al. [3]

☞ **EMFI** pour contourner un mécanisme anti-rejeu

✓ Matériel abordable

✗ possible altération des données



Avantages :

✓ L'injection de faute permet de contourner certains défis de l'extraction de données [3] [6].

Inconvénient :

✗ Risque d'altération des données [3] [5].

✗ Niveau technique requis [2] [5]

Sommaire

Conclusion

- ☞ Réflexion à un cadre législatif européen
- ☞ Des preuves de concepts prometteuse

Conclusion

- ☞ Réflexion à un cadre législatif européen
- ☞ Des preuves de concepts prometteuse

- ☞ Des pré-requis techniques important
- ☞ Des matériels onéreux

Conclusion

- ☞ Réflexion à un cadre législatif européen
- ☞ Des preuves de concepts prometteuse

- ☞ Des pré-requis techniques important
- ☞ Des matériels onéreux

☞ **A ce jour ces méthodes ne sont employés que par des organismes spécialisés**

Références

[1] *Criminalistique numérique*. URL : https://www.interpol.int/fr/Notre-action/Innovation/Criminalistique-numerique (visité le 30/09/2024).

[2] Louis Dureuil. "Analyse de code et processus d'évaluation des composants sécurisés contre l'injection de faute". fr. Thèse de doct. Communauté Université Grenoble Alpes, oct. 2016. URL : https://theses.hal.science/tel-01403749 (visité le 30/09/2024).

[3] Aya Fukami et Richard Buurke. "Keyless Entry : Breaking and Entering eMMC RPMB with EMFI". In : *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. WiSec '24. New York, NY, USA : Association for Computing Machinery, mai 2024, p. 145-155. ISBN : 9798400705823. DOI : 10.1145/3643833.3656114. URL : https://dl.acm.org/doi/10.1145/3643833.3656114 (visité le 30/05/2024).

Références

[4] Aya Fukami, Radina Stoykova et Zeno Geradts. “A new model for forensic data extraction from encrypted mobile devices”. In : *Forensic Science International : Digital Investigation* (sept. 2021). doi : 10.1016/j.fsidi.2021.301169. url : https://linkinghub.elsevier.com/retrieve/pii/S2666281721000779 (visité le 19/06/2023).

[5] Carlton Shepherd et al. “Physical fault injection and side-channel attacks on mobile devices : A comprehensive analysis”. In : *Computers & Security* 111 (1er déc. 2021). issn : 0167-4048. doi : 10.1016/j.cose.2021.102471. url : https://www.sciencedirect.com/science/article/pii/S0167404821002959 (visité le 30/09/2024).

[6] Aurélien Vasselle et al. “Laser-Induced Fault Injection on Smartphone Bypassing the Secure Boot”. In : *2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. Sept. 2017. doi : 10.1109/FDTC.2017.18. url : https://ieeexplore.ieee.org/document/8167709 (visité le 18/10/2023).