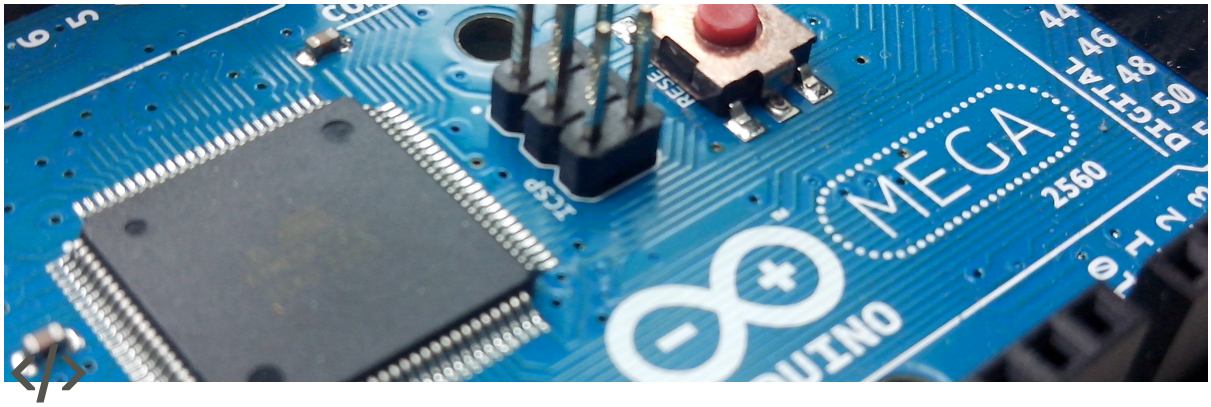

ESC 2023 - Hackcess

Rapport sur les Attaques par Canaux Cachés

Table des matières :

1 - Introduction

1-1 Contexte du rapport

Il est essentiel de noter que ce rapport est basé sur une recherche documentaire approfondie effectuée en utilisant les nombreuses ressources disponibles sur le web et dans le cadre de la compétition ESC. Notre objectif est de compiler et de synthétiser les informations pertinentes concernant les attaques par canaux cachés à partir de sources fiables et crédibles.

L'objectif principal en participant à cette compétition est de renforcer nos compétences en cybersécurité et d'acquérir une expérience dans les attaques par canaux cachés.

1-2 Objectifs et portée du rapport

Ce rapport va permettre de fournir des explications sur les attaques par canaux cachés dans le domaine de la cybersécurité. Les objectifs spécifiques sont les suivants :

1. **Comprendre les Principes Fondamentaux :** Ce rapport vise à expliquer en détail les principes de base des attaques par canaux cachés, y compris leur définition, leur fonctionnement.

2. **Identifier les Principales Attaques :** Nous examinerons les différentes techniques et méthodes d'attaques par canaux cachés, en mettant en évidence des exemples concrets pour illustrer chacune d'entre elles.
3. **Analyser les Contre-Mesures :** Nous explorons les mesures de prévention et de détection des attaques par canaux cachés, afin de comprendre comment les organisations peuvent se défendre contre de telles menaces.

Nous n'aborderons pas les aspects pratiques de la mise en œuvre des attaques, car cela n'entre pas dans le cadre du rapport. De plus, nous ne traiterons pas des aspects juridiques liés à l'utilisation des attaques par canaux cachés.

2 - Principes des Attaques par Canaux Cachés

Les attaques par canaux cachés représentent une classe unique de menaces en cybersécurité, caractérisée par leur capacité à exploiter des chemins de communication non conventionnels et souvent imperceptibles pour transmettre des informations confidentielles.

Le principe fondamental des attaques par canaux cachés réside dans l'utilisation de méthodes non conventionnelles pour transférer des informations entre deux entités, souvent sans être détecté par les mécanismes de sécurité traditionnels. Le terme "canal caché" fait référence à un moyen de communication qui exploite des vecteurs inattendus ou inaperçus pour transmettre des données confidentielles.

Voici les éléments clés du principe des attaques par canaux cachés :

1. **Transmission Subreptice**
2. **Utilisation de Canaux Non Conventionnels**
3. **Contournement des Mesures de Sécurité**
4. **Transfert d'Informations Confidentielles**
5. **Variété de Méthodes**

2-1 Définition des Canaux Cachés

Contrairement aux canaux de communication classiques, tels que les réseaux informatiques ou les connexions physiques, les canaux cachés exploitent des vecteurs inattendus, tels que des retards dans le temps d'accès à une ressource, des signaux électromagnétiques indésirables, ou même des fluctuations dans la consommation d'énergie.

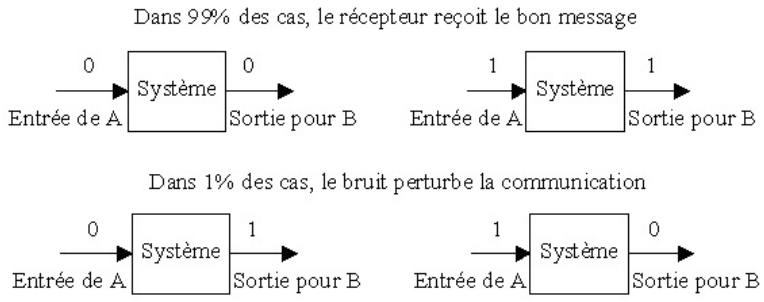

Figure 1 : Exemple fonctionnement canaux cachés

2-2 Raisons d’utiliser des Canaux Cachés

Voici les principales raisons d'utiliser ces attaques :

- **Contournement des Mécanismes de Sécurité :** Les canaux cachés permettent d'éviter la détection par les dispositifs de sécurité classiques, tels que les pare-feu.
- **Exfiltration Discrète de Données de manière furtive :** Ils offrent un moyen discret d'exfiltrer des données confidentielles d'un système sans attirer l'attention ou alerter des systèmes de défense

2-3 Fonctionnement des Canaux Cachés

Les méthodes courantes comprennent :

- **Canal de Stockage :** Des données sont cachées dans des zones de stockage, telles que la mémoire, le disque dur ou le registre de processeur.
- **Canal de Timing :** Les attaquants utilisent des écarts de temps entre les opérations pour transmettre des données. Par exemple, des retards dans l'accès à la mémoire peuvent être exploités.
- **Canal Acoustique :** Les bruits émis par le matériel informatique, tels que les disques durs ou les ventilateurs, sont utilisés pour transmettre des données.
- **Canal Électromagnétique :** Les variations dans les émissions électromagnétiques générées par le matériel sont exploitées pour transmettre des données.
- **Canal Réseau :** Des protocoles réseau sont manipulés pour envoyer des données dans des champs qui ne sont normalement pas utilisés à cette fin.
- **Canal Optique** : Des signaux lumineux sont utilisés afin de pertuber le fonctionnemment au niveau hardware pouvant ensuite provoquer un comportement inhabituel au niveau système.

3 - Principales Attaques par Canaux Cachés

3-1 Types d'Attaques

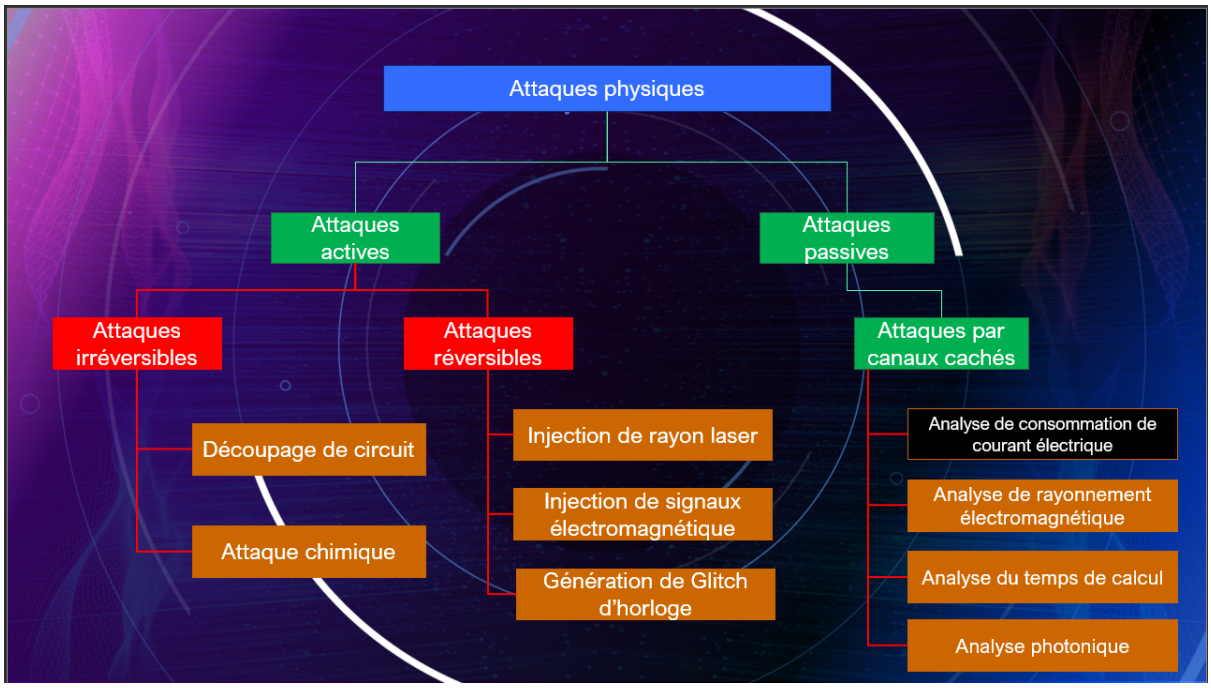

Figure 2 : Schéma types d’attaques

- Les **attaques passives** où on « écoute » seulement
  les fuites de ces canaux cachés (son, temps, ondes électromagnétiques, etc) d’ordinateurs, serveurs, microprocesseurs et ces attaques ne peuvent donc pas être détectées : dans certains cas cela peut se faire à grande distance (sur internet).

  Exemple : Écoute (Sniffing) d'un Canal Caché

  Supposons qu'un attaquant ait réussi à introduire un canal caché dans un réseau informatique. Ce canal caché utilise des variations subtils de la latence des paquets réseau pour transmettre des informations secrètes entre deux points. L'attaquant peut simplement écouter le trafic sur le réseau sans perturber son fonctionnement. Il collecte ainsi les données transmises via ce canal caché sans interagir activement avec lui.

  Les attaques passives sont généralement plus discrètes que les attaques actives, car elles n'interfèrent pas directement avec le fonctionnement du système cible. Cependant, elles peuvent être tout aussi préjudiciables en termes de vol d'informations sensibles.

  On peut également analyser le code Asssembleur d’un binaire qui fait fuiter des informations de manière non “voulue” (exemple : le temps de vérification d’un mot de passe entré) de sorte à identifier les sections les plus vulnérables du programme comme par exemple ici celles surlignées en rouge et ainsi les utiliser à notre guise pour retrouver des informations censées être chiffrées:

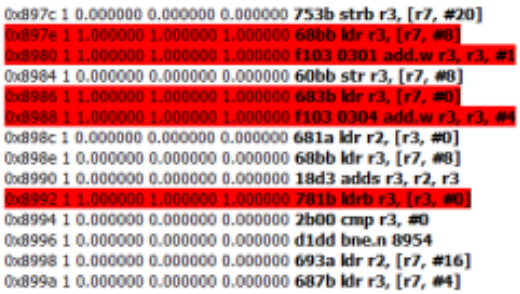

Figure 3 : Analyse statique de binaire

- les **attaques actives** avec diverses méthodes d’injection (lumière, chaleur, laser, ondes, etc) pour engendrer des fautes transitoires ou permanentes qui perturbent les résultats des calculs.

  Par exemple, ils pourraient moduler la fréquence de transmission dans un canal caché pour transmettre des données secrètes.

  Le principal but est de capter les informations indirectes qui donneront, après transformations et calculs, la clé secrète convoitée. Ici, il faudra avoir accès ou être proche de l’objet attaqué mais c’est bien sûr possible pour beaucoup d’objets dans la nature (carte à puce, IoT, etc).

3-2 Les Attaques Acoustiques

Selon nos recherches, Asonov et Agrawal ont été parmi les premiers chercheurs à publier une attaque concrète exploitant les émanations acoustiques des claviers (Asonov et Agrawal, 2004). Ils ont observé que le son émis lors de la frappe des touches diffère légèrement d'une touche à l'autre. Dans leur étude (voir 6 - Références) , ils ont élaboré une méthode précise pour récupérer des informations à partir des sons générés par les frappes sur un clavier, en utilisant des réseaux de neurones comme classificateurs acoustiques.

Leur approche a consisté à apprendre aux réseaux de neurones à reconnaître les sons associés à chaque touche. Pour ce faire, ils ont enregistré 100 frappes de chaque touche, associant chaque échantillon sonore à l'étiquette correspondante (la touche en cours de saisie). Les données sonores brutes ont ensuite été numérisées et transformées

en vecteurs à l'aide de la fonction de transformation de Fourier rapide (FFT). Une fois les réseaux de neurones formés, ils ont été en mesure de reconnaître efficacement les frappes ultérieures sur le clavier.

Cette recherche a mis en évidence une vulnérabilité potentielle dans les systèmes de sécurité, car elle suggère qu'un attaquant pourrait potentiellement intercepter des données sensibles en utilisant des microphones cachés pour enregistrer les sons du clavier, même sans accès direct à l'ordinateur cible. Depuis lors, cette idée a conduit au développement de contre-mesures, notamment des logiciels de suppression de bruit et des claviers silencieux conçus pour minimiser les émanations acoustiques, afin de réduire le risque de telles attaques.

3-3 Les Attaques Optiques

D'après une étude de Sergei P. Skorobogatov et Ross J. Anderson, la projection d'un laser dans un transistor cible peut causer un défaut transitoire et ainsi provoquer un comportement habituel dans des process cryptographiques, des protocols et même dans le flux de control du processeur. Lors de leurs recherches, ils ont notament reussi a modifier et reinitialiser la SRAM d'un microcontrolleur à l'aide d'un équipement laser très peu couteux et accessible au publique.

Cette recherche, associé à de nombreuses précédentes, confirme une vulnérabilité flagrante dans les canaux optiques pouvant ainsi pertuber le fonctionnement correct d'un système.

4 - Contre-Mesures

- Amélioration des composants électroniques pour réduire leurs émissions (meilleurs matériaux, designs dédiés…)
- Isolation des équipements sensibles :
  - Ordinateurs hors réseau (stratégie du *air-gapping*)
  - Systèmes d'isolation électromagnétique type cages de Faraday
  - Création de chambres fortes isolées : réseaux électriques séparés, isolation des câbles, ….
  - Blindage matériel sur les boitiers d'ordinateurs, fenêtre, cloisons, …
  - Utilisation de fibre optique (ne provoque que très peu d'émissions résiduelles)
- Procédures liés aux interactions avec des personnes :
  - Suppression d'éventuels appareils électroniques pouvant servir à capter des signaux :
    - Retirer les micros en place par défaut sur les ordinateurs (vu chez Mark Zuckerberg !)
    - Interdiction des téléphones portables (bases militaires, cérémonies des clés)
  - Protection lors de l'entrée d'un mot de passe (cf. Edward Snowden sous sa couette, visible dans le film éponyme)
- Meilleur design des algorithmes cryptographiques utilisés, afin de rendre moins reconnaissables les opérations effectuées (paramètre inclus dans le cahier des charges du concours qui donna naissance à l'algorithme AES)
- Émission de bruit blanc
- Introduction d'une part d'aléatoire dans l'ordre de traitement des opérations dans un processeur
- Introduction d'étapes « inutiles » dans les étapes de calcul afin de brouiller les pistes.
- Architectures de processeurs asynchrones afin de rendre plus difficile la corrélation des traitements du processeur

5 - Conclusion

En conclusion, les attaques par canaux cachés représentent une catégorie unique de menaces en cybersécurité qui exploitent des chemins de communication non conventionnels pour transmettre des informations secrètes ou malveillantes.

Comme nous l'avons exploré tout au long de ce rapport, ces attaques peuvent prendre de nombreuses formes, allant des canaux acoustiques aux canaux de timing, en passant par les canaux de stockage, et peuvent être utilisées pour contourner les mécanismes de sécurité traditionnels.

L'utilisation de canaux cachés est souvent motivée par le désir de communication clandestine, la discrétion dans l'exfiltration de données sensibles ou la perturbation subtile d'un système. Cependant, il est important de noter que l'utilisation de ces techniques pour des activités malveillantes est illégale et condamnable.

Heureusement, des contre-mesures existent pour détecter et prévenir les attaques par canaux cachés. Ces contre-mesures incluent l'amélioration de la sécurité matérielle, l'isolation des équipements sensibles, la protection des procédures d'interaction avec les personnes, l'amélioration des algorithmes cryptographiques, l'émission de bruit blanc, l'introduction d'aléatoire dans le traitement des opérations, et l'adoption d'architectures de processeurs asynchrones.

En participant à cette compétition et en menant des recherches approfondies sur les attaques par canaux cachés, nous avons acquis une compréhension approfondie de cette menace et des moyens de la contrer. Il est essentiel de poursuivre notre vigilance et notre engagement envers la cybersécurité pour protéger nos systèmes et nos données contre ces attaques insidieuses.

En fin de compte, la cybersécurité est une préoccupation constante et en constante évolution, et la compréhension des canaux cachés fait partie intégrante de la défense contre les menaces actuelles et futures. Nous espérons que ce rapport a contribué à sensibiliser davantage à cette question complexe et à inspirer une réflexion continue sur la sécurité informatique.

6 - Références

https://people.eecs.berkeley.edu/~tygar/papers/Keyboard_Acoustic_Emanations_Revisited/tiss.preprint.pdf

https://www.cl.cam.ac.uk/~sps32/ches02-optofault.pdf

Attaques par canaux auxiliaires

Elles portent dans la majorité des cas sur l'extraction d'informations relevant de la cryptographie, clés de chiffrement ou des vecteurs d'initialisation.

https://www.synetis.com/attaques_auxiliaires/

Lundi Cybersécurité : Attaques par canaux | Devinci Executive Education

La cybersécurité et les attaques par canaux, Jean-Jacques Quisquater, cryptologue belge, vous en parle dans cette édition.

https://executive.devinci.fr/lundi-de-la-cybersecurite-attaques-par-canaux-caches/

Attaques par canaux cachés INF Sécurité des systèmes informatiques Hiver ppt télécharger

Introduction Une nouvelle catégorie d'attaques qui vise le matériel qui implémente les algorithmes cryptographiques a vu le jour dans les années 90, chose qui a obligé les concepteurs des circuits intégrés a prendre en considération un ensemble de mesures pour contrer ces attaques et renforcer la sécurité des systèmes cryptographiques.

https://slideplayer.fr/slide/16650397/

SLEAK: A Side-channel Leakage Evaluator and Analysis Kit | MITRE

Side-channel attacks (SCA) present a major threat to secure embedded systems. In this paper, the authors present a new technique for testing software for SCA vulnerabilities in a fast, inexpensive, and automated manner.

https://www.mitre.org/news-insights/publication/sleak-side-channel-leakage-evaluator-and-analysis-kit

11-22 : "Lundi de la Cyber": "Les attaques par canaux cachés" par Jean-Jacques Quisquater et David Samyde

Cette conférence des "Lundi de la Cyber porte sur: * les attaques passives où on "écoute" seulement les fuites de ces canaux cachés (son, temps, ondes électromagnétiques, etc) ; * les attaques actives avec diverses méthodes d'injection (lumière, chaleur, laser, faisceau de cyclotron, ondes électromagnétiques, utilisation des protocoles, etc).

https://www.dailymotion.com/video/x8fx6rb

Réalisé par :

- Skairik
- Successful
- Jadblow
- Rico9
- m0