ESC 2024 - Rapport sur les Attaques par Canaux Cachés applicable aux CPS

Par :
Hypno
Tensheli
Alvi
Gmx.0x1

Sommaire :

1 - Introduction

1-1/ Contexte du rapport

Il est important de retenir que ce rapport est basé sur des recherches documentaires poussées effectuées sur le web afin de rendre un rapport le plus complet pour la compétition CSAW ESC2024.

Dans ce rapport, notre objectif était de synthétiser et joindre les informations pertinentes concernant les attaques par canaux cachés en nous appuyant de source fiable. De plus, l'objectif de notre équipe est d'approfondir et de renforcer nos compétences en cybersécurité et dans ce cadre acquérir des compétences dans les attaques par canaux cachés.

1-2/ Objectifs du rapport

Ce rapport vise à fournir des éclaircissements sur les attaques par canaux cachés dans le domaine de la cybersécurité. Nous allons aussi nous concentrer sur 3 points qui sont :

1. Comprendre les fondamentaux de ces attaques:

Notre rapport visera à expliquer précisément le principe de base des attaques par canaux cachés en nous intéressant aux définitions mais aussi au fonctionnement de ces attaques.

2. Identifier les principales attaques :

Nous nous intéresserons principalement aux différents types d'attaques possibles en se concentrant sur la technique et la méthode pour les réaliser. Nous mettrons donc en avant 2 exemples afin d'expliquer concrètement leur fonctionnement.

3. Analyser et proposer des atténuations intéressantes :

Nous finirons par nous intéresser aux différentes mesures de prévention et de protection que nous pouvons mettre en place pour

diminuer et détecter ces attaques par canaux cachés pour comprendre comment les organisations peuvent se défendre contre ce type de menaces.

Cependant, nous resterons plutôt vague et nous n'aborderons pas certaine partie importante comme l'aspect juridique car cela n'entre pas dans le cadre de notre rapport.

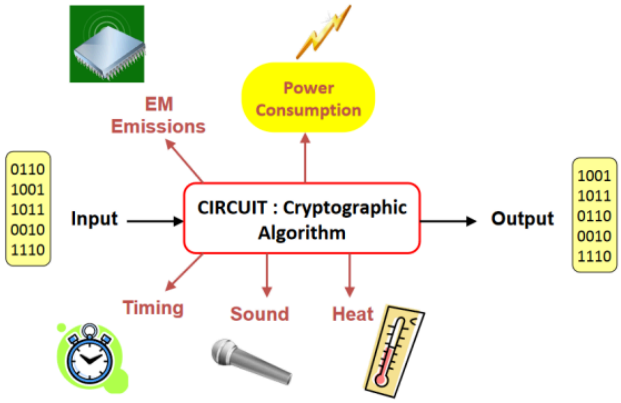
2 - Généralités des Attaques par Canaux Cachés

Les attaques par canaux cachés représentent une classe unique de menace en cybersécurité. Il est caractérisé par l'exploitation des chemins de communication non-conventionnel et la plupart du temps imperceptible pour transmettre des informations spécifiques. Le principe fondamental des attaques par canaux cachés repose sur l'utilisation de méthodes non conventionnelles afin de transférer des données entre deux entités en étant la plupart du temps non détectées par les systèmes de sécurité. 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. Utilisation de Canaux Non Conventionnels
- 2. Transfert d'Informations Confidentielles
- 3. Contournement des Mesures de Sécurité
- 4. Variété de Méthodes
- 5. Transmission Subreptice

2-1/ Définition

A la différence des moyens de communication standard (réseau informatique, LAN …) Les canaux cachés exploitent des vecteurs et des failles inattendus tels que les signaux électromagnétiques, des retards dans le temps mais aussi la fluctuation de la consommation d'énergie.



2-2/ Raisons de les utiliser

Voici les principales raisons d'utiliser ces attaques :

Exfiltration discrète voire presque invisible de données : Ces attaques offrent un moyen discret d'exfiltrer des données d'un système sans que celui-ci s'alerte ou alerte les systèmes de défense.

Contournement d'un système de sécurité : Les attaques par canaux cachés permettent d'esquiver des systèmes de sécurité courant tels que les pare-feu .

2-3/ Fonctionnement

Les méthodes d'attaques courantes comprennent :

- Canal de Stockage : Des données sont cachées dans des stockages, comme la mémoire vive, le processeur …

- Canal Optique : Des signaux lumineux sont émis afin de perturber le fonctionnement ce qui peut entraîner un comportement inhabituel du système.

- Canal Électromagnétique : Des émissions électromagnétiques générées par le matériel sont exploitées afin de récupérer et transmettre des données.

- Canal Réseau : Des protocoles réseau sont altérés pour envoyer des données qui ne sont normalement pas utilisés à cette fin.

- Canal Acoustique : Les bruits produits par le matériel informatique sont utilisés pour transmettre des données.

3 - Principales Attaques par Canaux Cachés

3-1 Types d'Attaques

Tout d'abord, ce type d'attaque est dite "non invasive". C'est-à-dire qu'elle ne va pas altérer le fonctionnement normal de la victime. Généralement, il s'agit d'attaques passives. C'est à dire qu'on écoute les fuites de données des canaux (son, temps, ondes …) émanant d'un système informatique. Ce type d'attaque peuvent même se faire à longue distance.

Exemple : Sniffing d'un Canal Caché

Imaginons qu'un attaquant ait réussi à intégrer un canal caché dans le système informatique. Ce canal pourra donc utiliser par exemple des variations subtiles des paquets réseaux dans le but de transmettre des informations secrètes (attaque man in the middle). Cependant, l'attaquant peut aussi écouter simplement le trafic afin d'extraire des données sans modifier ni altérer le fonctionnement du réseau et en étant parfaitement invisible.
Ainsi, ces attaques passives, souvent réputées discrètes , n'interfèrent pas avec le bon fonctionnement du réseau alors qu'elles peuvent être tout aussi dangereuses car elles sont invisibles ou presque.

Un autre type d'attaque possible est l'attaque active. Celle-ci est plus invasive et utilisera diverses méthodes d'injection (lumière, ondes, etc) afin de provoquer des erreurs de calcul permanentes ou non.

Par exemple, un pirate pourrait moduler un signal afin d'exfiltrer des données secrètes. Le principal but est de capter les informations indirectes qui donneront, après transformations et calculs, la clé secrète convoitée. Dans ce genre d'attaque, il faut avoir un accès physique avec l'objet cible.

3-2 Les Attaques Électromagnétique

Ces attaques visent les émissions électromagnétiques des composants afin d'en soutirer des informations.
Ce type d'attaque ne nécessite pas d'intrusion ni de modification, seulement d'avoir la machine à attaquer à portée de main. On utilise une sonde électromagnétique pour capter les radiations électromagnétiques pour ensuite les traiter afin de voler des informations. Ces attaques sont compliquées à détecter étant donné qu'on agit à l'extérieur de la machine.

On peut tenter d'interpréter directement les données traitées ou alors établir des statistiques avec des données obtenues pour essayer d'être plus précis.

4 - Atténuations possibles

Afin de limiter ce genre d'attaque et de rendre nos systèmes plus sécurisé, plusieurs contre-mesures ou atténuations sont possible tel que :

- Isolation des équipements sensibles : Il est possible afin de limiter les fuites de données de mettre les ordinateurs hors réseau, de mettre en place un système d'isolation électromagnétique, de créer une chambres fortes isolées c'est-à-dire avec un réseau électrique séparé ….

- Interdiction des téléphones portables dans les sites à données sensibles (bases militaires)

- Meilleur design des algorithmes cryptographiques utilisés, afin de rendre moins reconnaissables les opérations effectuées

- Émission de bruit blanc afin de gêner le bruit des canaux.

- Architectures de processeurs asynchrones afin de rendre plus difficile la corrélation des traitements du processeur

5 - Conclusion

Pour conclure notre rapport, les attaques par canaux cachés représentent une catégorie spéciale de menaces en cybersécurité. Elles exploitent des chemins de communication spécifiques pour transmettre ou récupérer des informations secrètes.
Comme nous avons pu le découvrir tout au long de notre rapport, ces attaques peuvent se manifester sous de nombreuses formes en partant des attaques par canaux acoustiques pour continuer vers les attaques par canaux réseau pour finir par les attaques sur les canaux de stockage. Ces attaques ont pour but d'être plus discrètes afin de ne pas attirer l'attention des outils de sécurité classique.

L'utilisation de ce type d'attaque est généralement motivée par un désir de communication clandestine, la discrétion dans l'exfiltration de données sensibles ou la perturbation subtile d'un système.

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

Il convient de noter que l'utilisation de ces méthodes à des fins malveillantes est non seulement répréhensible, mais aussi lourdement punie.

Heureusement, des mesures efficaces ont été mises en œuvre afin de repérer et faire face aux attaques par le biais de canaux dissimulés. La sécurité matérielle est renforcée, les systèmes critiques sont isolés, les processus d'interaction humaine sont protégés, les algorithmes cryptographiques sont améliorés, l'utilisation de bruit blanc est possible, la variabilité est introduite dans le traitement des opérations et les processeurs sont asynchrones.

Nous avons acquis des connaissances solides dans ce domaine grâce à notre participation à cette compétition et à nos études approfondies sur les attaques par des canaux cachés.

Enfin, la cybersécurité reste un défi constant avec une évolution continuelle. Il est essentiel de comprendre les canaux cachés afin de les saisir.

6- Sources :

https://www.synetis.com/attaques_auxiliaires/
https://www.centexbel.be/fr/node/1265
https://www.worldscientific.com/doi/abs/10.1142/S2424862217500142
https://www.lirmm.fr/~rouzeyre/PDF/Crypto/AttaquesCanauxCaches.pdf
https://fr.wikipedia.org/wiki/Attaque_par_canal_auxiliaire
https://www.synetis.com/attaques_auxiliaires/
http://www.goubin.fr/papers/attaques-side-channel.pdf
https://www.arcsi.fr/doc/Lettre-Lundi-Cyber-No53.pdf
https://csrc.nist.gov/csrc/media/events/physical-security-testing-workshop/documents/papers/physecpaper19.pdf
https://www.lemondeinformatique.fr/actualites/lire-si-industriels-embarques-zoom-sur-les-attaques-et-moyens-de-contournement-76510.html
https://fr.wikipedia.org/wiki/Analyse_d'émanations_électromagnétiques /
https://en.wikipedia.org/wiki/Electromagnetic_pulse
https://www.mitre.org/news-insights/impact-story/electromagnetic-pulse-dangerous-overlooked-threat
https://www.cisa.gov/topics/cyber-threats-and-advisories
https://www.eccouncil.org/cybersecurity-exchange/network-security/how-to-prevent-network-security-attacks/