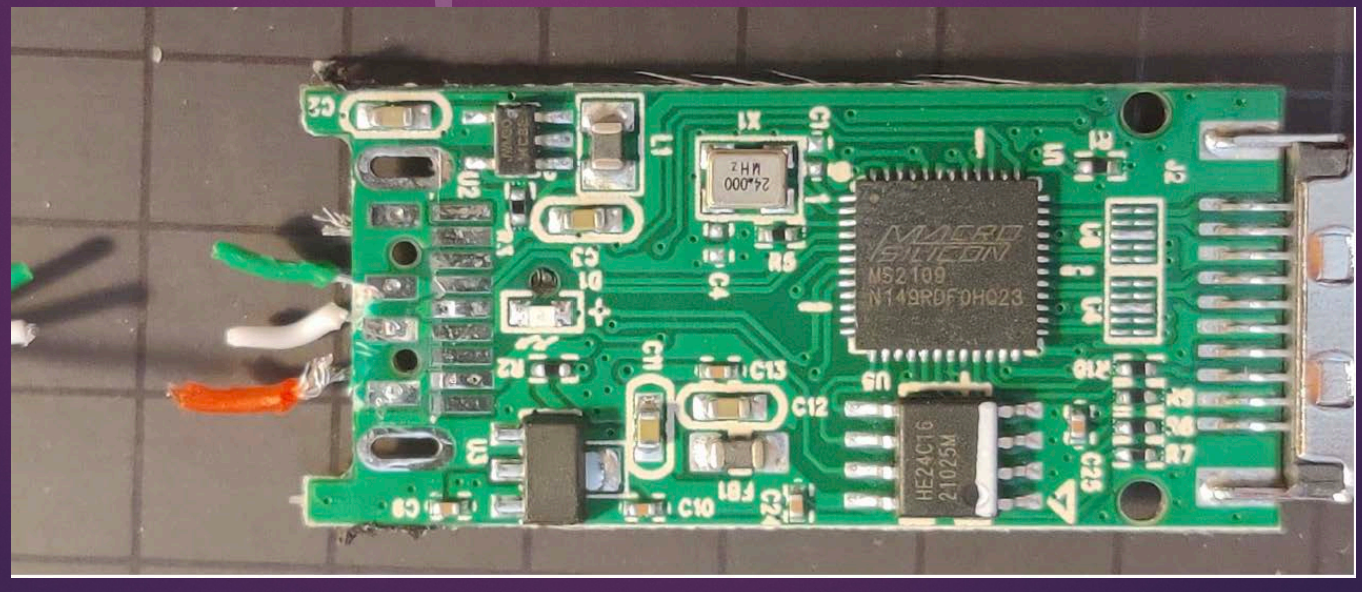
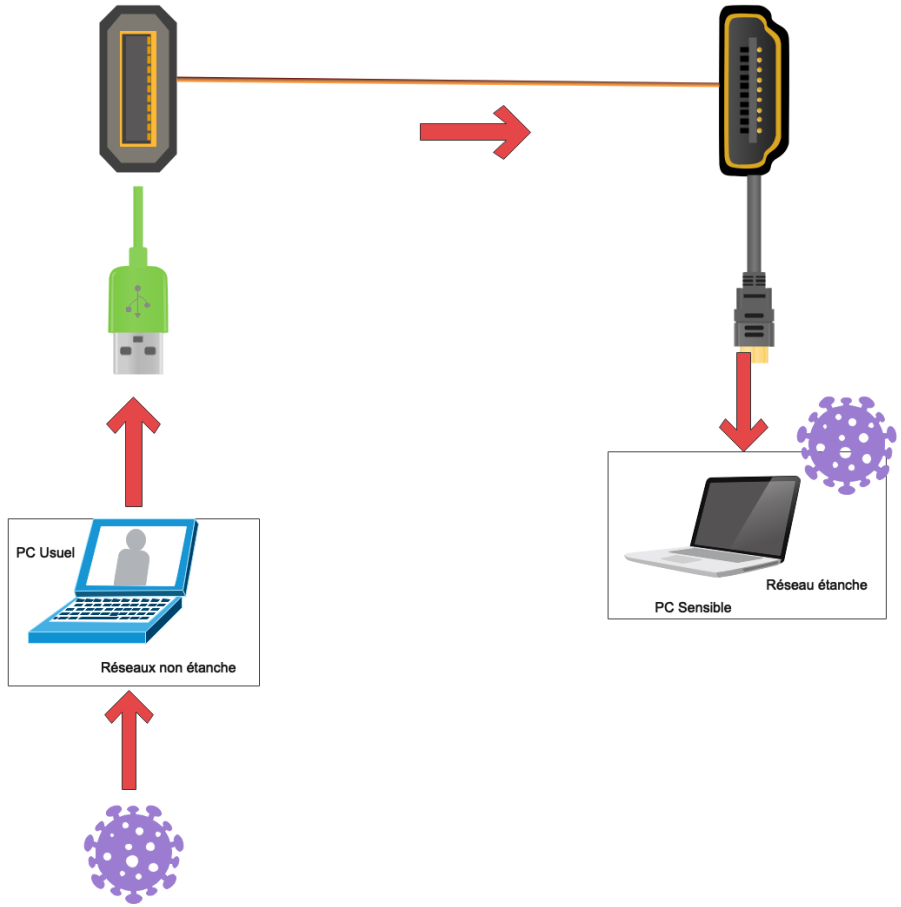
Recherche de vulnérabilités dans un adaptateur USB HDMI



Scénario

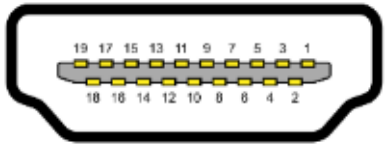
- **Postulat de départ :**
- PC sensible sous Windows ou Linux dans un environnement étanche.
- Souhait de diffuser une recopie vidéo vers un autre PC sous Windows dans un environnement non protégé et potentiellement infecté.
- **Configuration :**
- Connexion des deux PC via un adaptateur HDMI femelle (côté PC sensible) - (côté PC non protégé) pour le transfert de l'image

Scénario



La norme HDMI 1.14b

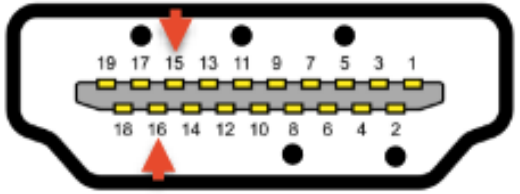
- HDMI 1.14b (la plus courante) contient 19 fils.



1 : TMDS Data2+	2 : Shield 2	3 : TMDS Data2-	4 : TMDS Data1+	5 : Shield 1
6 : TMDS Data1-	7 : TMDS Data0+	8 : Shield 0	9 : TMDS Data0-	10 : TMDS Clock+
11 : Shield Clock	12 : TMDS Clock-	13 : CEC	14 : HEAC+	15 : DDC (I²C SCL)
16 : DDC (I²C SDA)	17 : GND	18 : +5V	19 : Hot plug/HEAC-/MHL CBUS	

Le DDC, pour Display Data Channel.

Bus bidirectionnel I2C qui va récupérer différents éléments du moniteur sur lequel il va se connecter.



- EDID (Extended Display Identification Data)

- Il s'agit d'une mémoire flash qui contient la structure de donnée que va décrire l'écran.

  Normalement seulement accessible en lecture mais certaines attaques ont pu prouver qu'il est parfois possible de réécrire dans espace mémoire.

Le DDC, pour Display Data Channel.

- Seuls certains écrans étaient vulnérables, et servaient de relais pour l'attaque.

Ces écrans avaient besoin de récupérer les paramètres des flux vidéo, et étaient donc dans certains cas sensibles à une réécriture.

- Dans le cas d'un pc portable, l'écran ne récupère pas ces informations car elles sont codées en dur au niveau hardware.
On peut modifier l'EDID depuis le pc portable, mais pas via la connexion HDMI.

-
- - Le convertisseur ne permet pas depuis l'interface USB d'interagir dans ce sens avec l'HDMI

- L'EDID ne présente à priori pas dans notre cas de surface visible d'attaque
  http://forum.notebookreview.com/threads/intel-optimus-display-overclocking.823648/

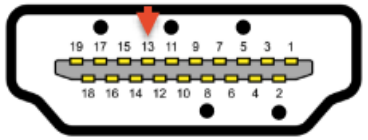
Le CEC, pour Consumer Electronics Control

Le CEC est un bus bidirectionnel qui permet de piloter les appareils

Contrôle One-Touch : Allumer tous les appareils avec une seule télécommande.

Contrôle du Playback : Contrôler la lecture de médias sur différents appareils.

Tuner Control : Choisir et contrôler des tuners de différents appareils.



OSD Naming : Nommer et renommer des appareils sur le réseau HDMI.

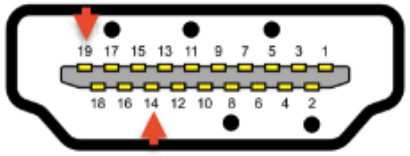
Routing du Signal : Changer l'entrée source sur un appareil de visualisation.

Exemples d'Utilisation :Un lecteur DVD peut allumer automatiquement une TV et sélectionner la bonne entrée HDMI.

Vecteur d’attaque le plus intuitif car il interagit avec les deux extrémités d’une connexion HDMI.

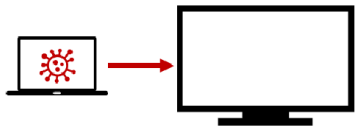
Le HEAC pour HDMI Eternet and Audio return channel

- C’est la grande innovation du HDMI 1.14b.
- flux Ethernet à une vitesse de 100mb/s à travers un cables HDMI.
  - Il sert à relier à internet via un périphérique centralisé (une TV connecté, un home station, un box etc), tous les équipements connectés via le cable sans avoir besoin de connecter un câble Ethernet en parallèle.



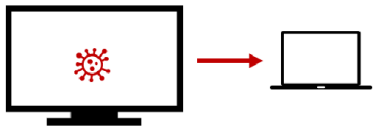
Exemples d'attaques via HDMI

- EDID Fuzzer : https://github.com/nccgroup/EDIDFuzzer (Andy Davis, Blackhat EU 2012)
  - Crash du driver Nvidia nvlddmkm.sys sous Windows 7
- Fuzzing CEC : Joshua Smith DEFCON 23 (2015)
  - Crash d'un téléviseur Panasonic via CEC
- Fuzzing CEC+EDID : Hyejin Jeong, DEFCON 27 (2019) (+Changhyeon Moon, HITB 2019)
  - Vulns CEC sur Android et EDID sur le driver i915 Ubuntu Linux
- Cinq CVE en 2017 dans le noyau Linux Android (trois EDID, deux CEC)
  - CVE-2017-{9689, 9719, 9722, 11030, 11093}
- Echange de données à travers d'un KVM (l'écran sert de support de stockage)
  - C.f. Protection Profile for Peripheral Sharing Switch, NIAP 2015



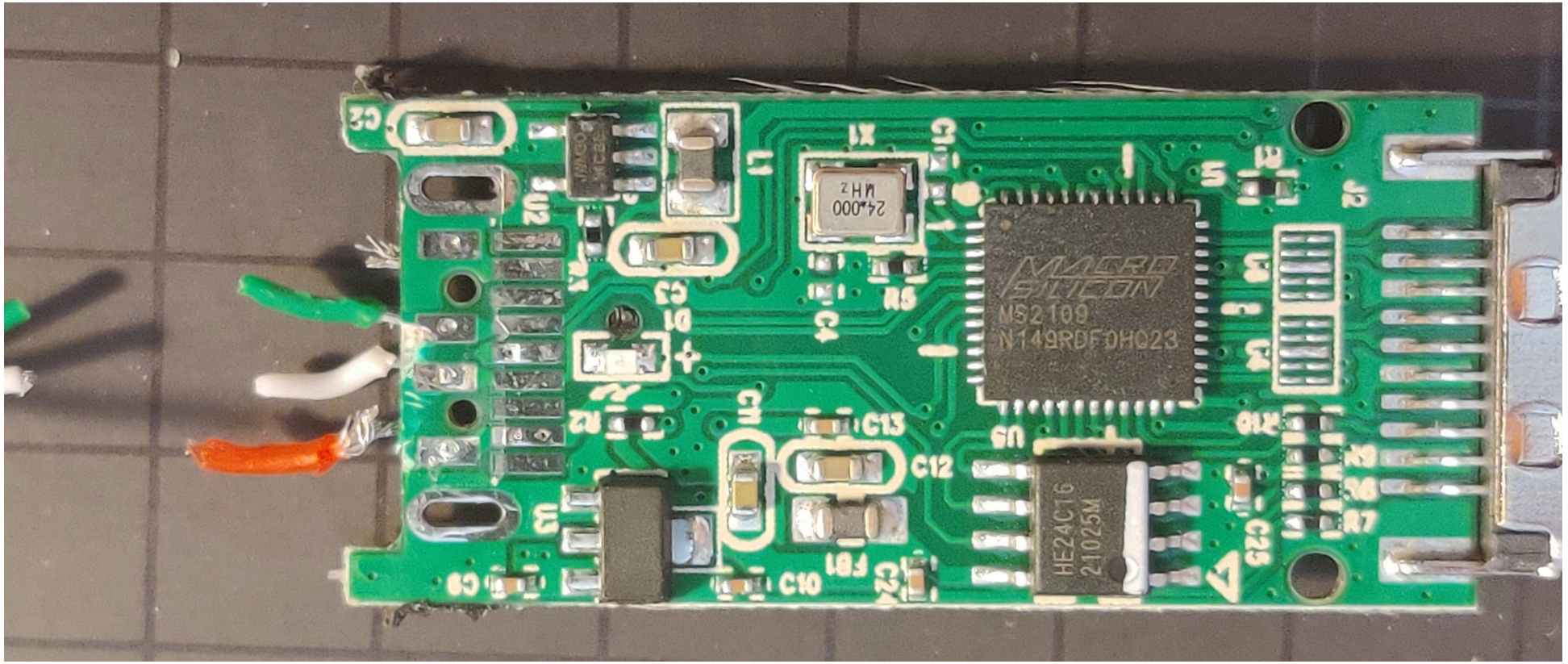
1: un ordinateur injecte un implant logique dans l'écran

2 : l'implant reste stocké dans l'écran



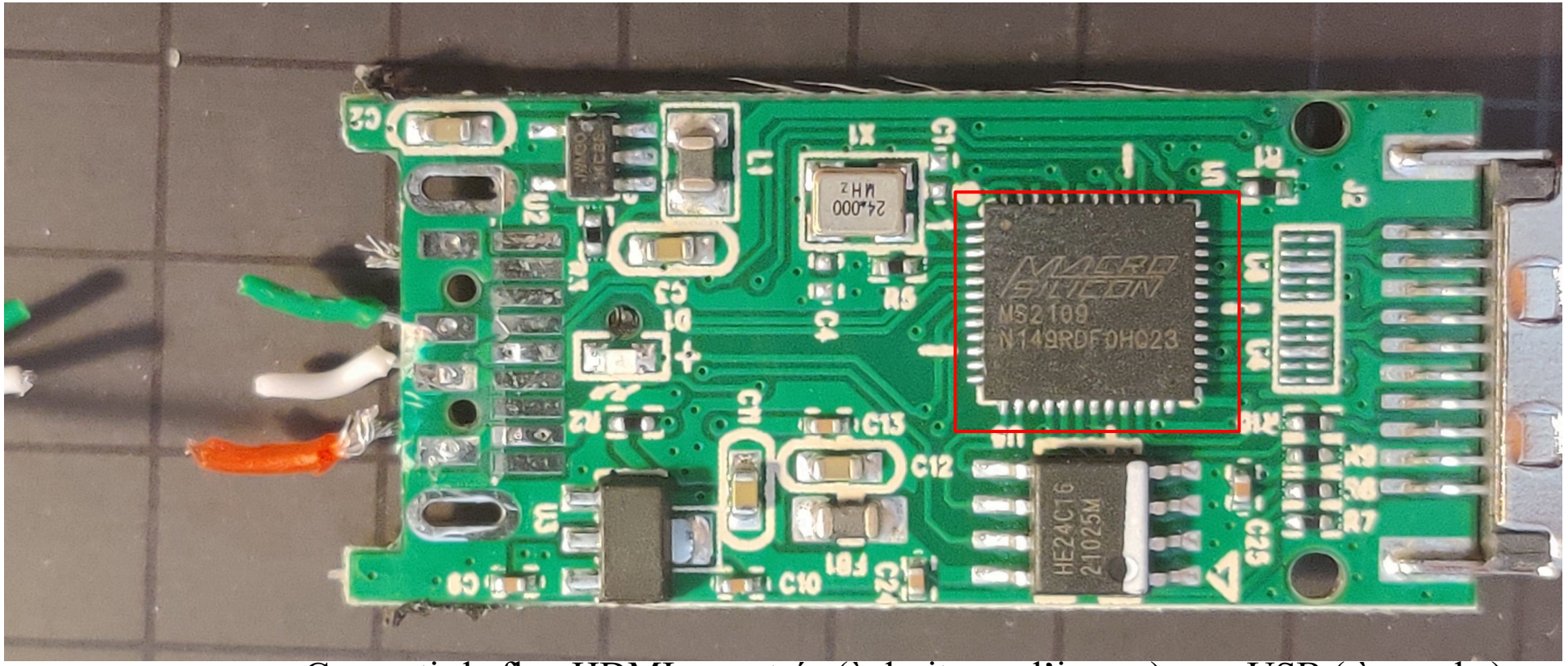
3 : l'implant déclenche une vulnérabilité qui compromet l'ordinateur qui y est branché

Analyse de l'adaptateur HDMI - USB



Analyse de l'adaptateur HDMI - USB

Macro Silicon MS2109



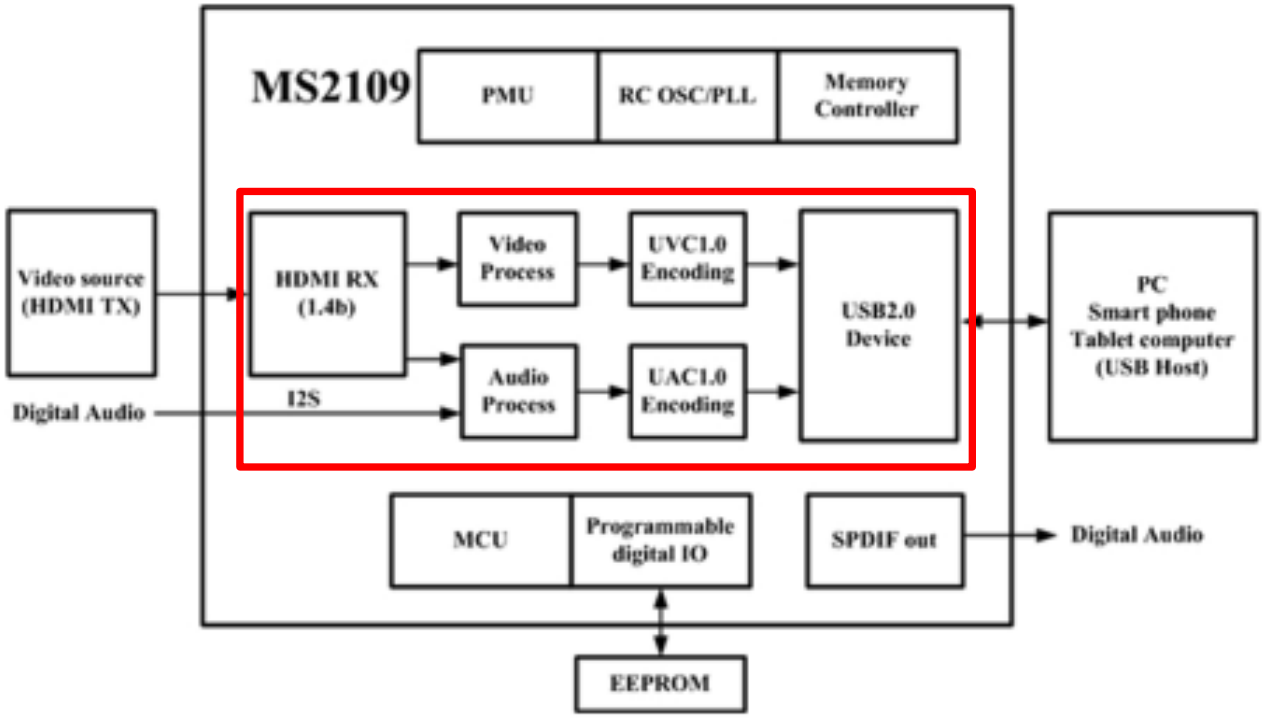
Convertir le flux HDMI en entrée (à droite sur l'image) vers USB (à gauche)

Analyse de l'adaptateur HDMI - USB

Macro Silicon MS2109

Function Block Diagram

Sens unidirectionnel du flux de l'HDMi vers l'USB

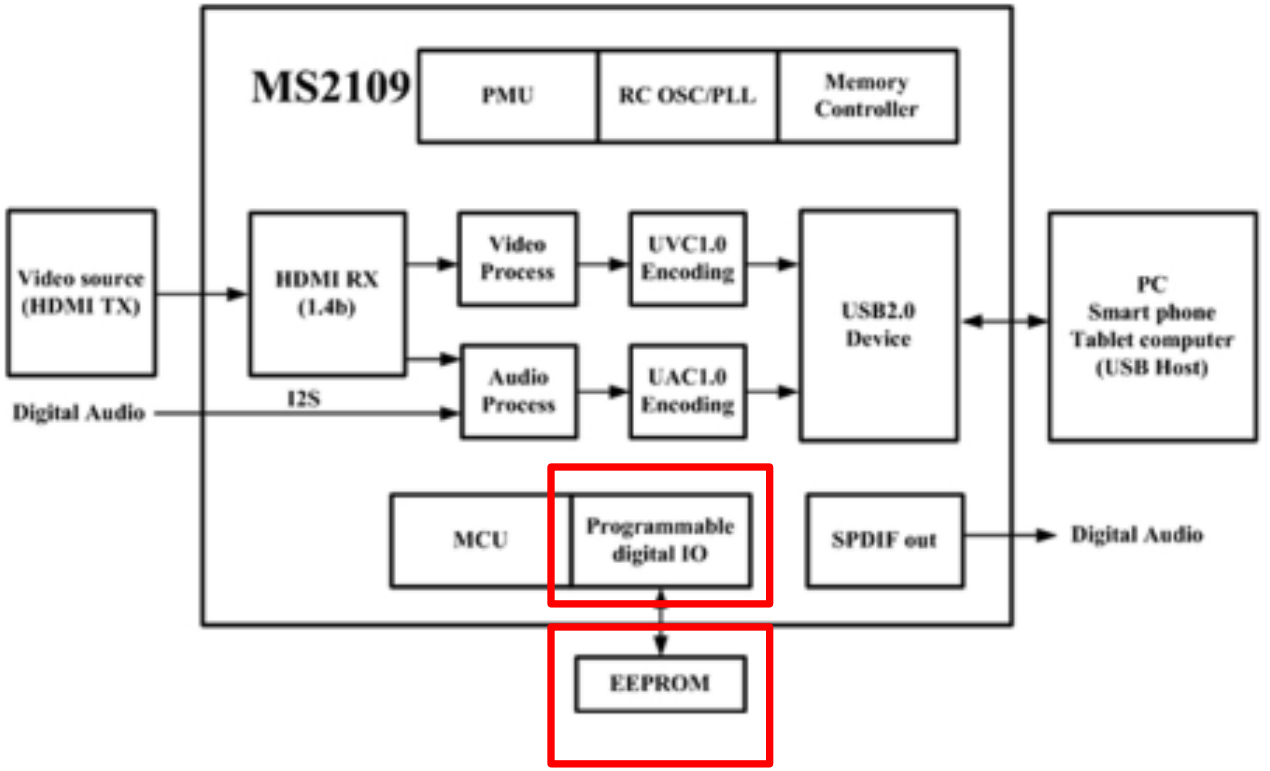


Analyse de l'adaptateur HDMI - USB

Macro Silicon MS2109

Function Block Diagram

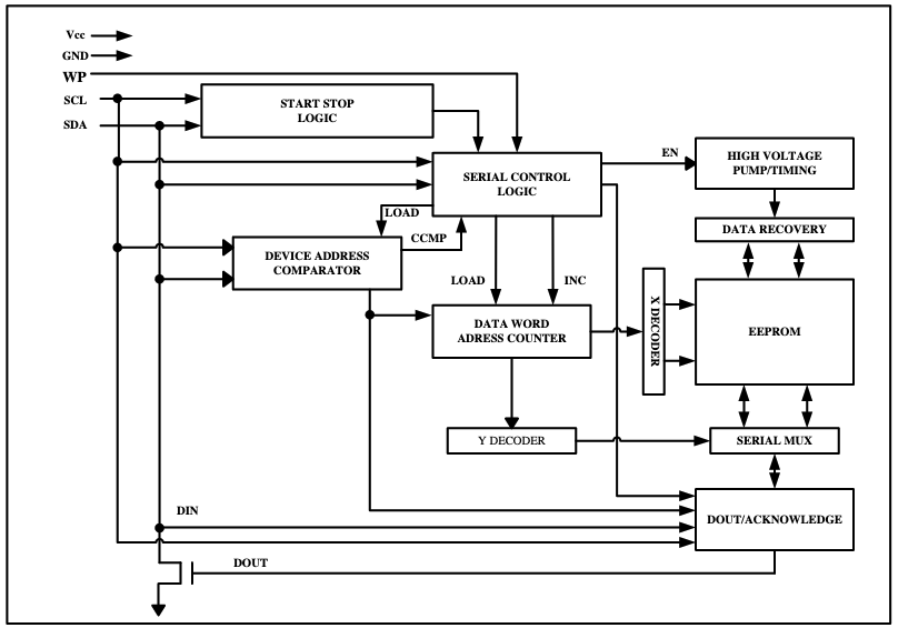
Sens unidirectionnel du flux de l'HDMi vers l'USB



Analyse de l'adaptateur HDMI - USB

EEPROM 24C16, un modèle assez standard.

Block Diagram



SERIAL DATA (SDA): The SDA pin is bi-directional for serial data transfer. This pin is open-drain driven and may be wire-ORed with any number of other open-drain or open-collector devices.

2000octets de mémoire sont disponibles en lecture et écriture et bidirectionnel

Analyse de l'adaptateur HDMI - USB

Dump de la mémoire

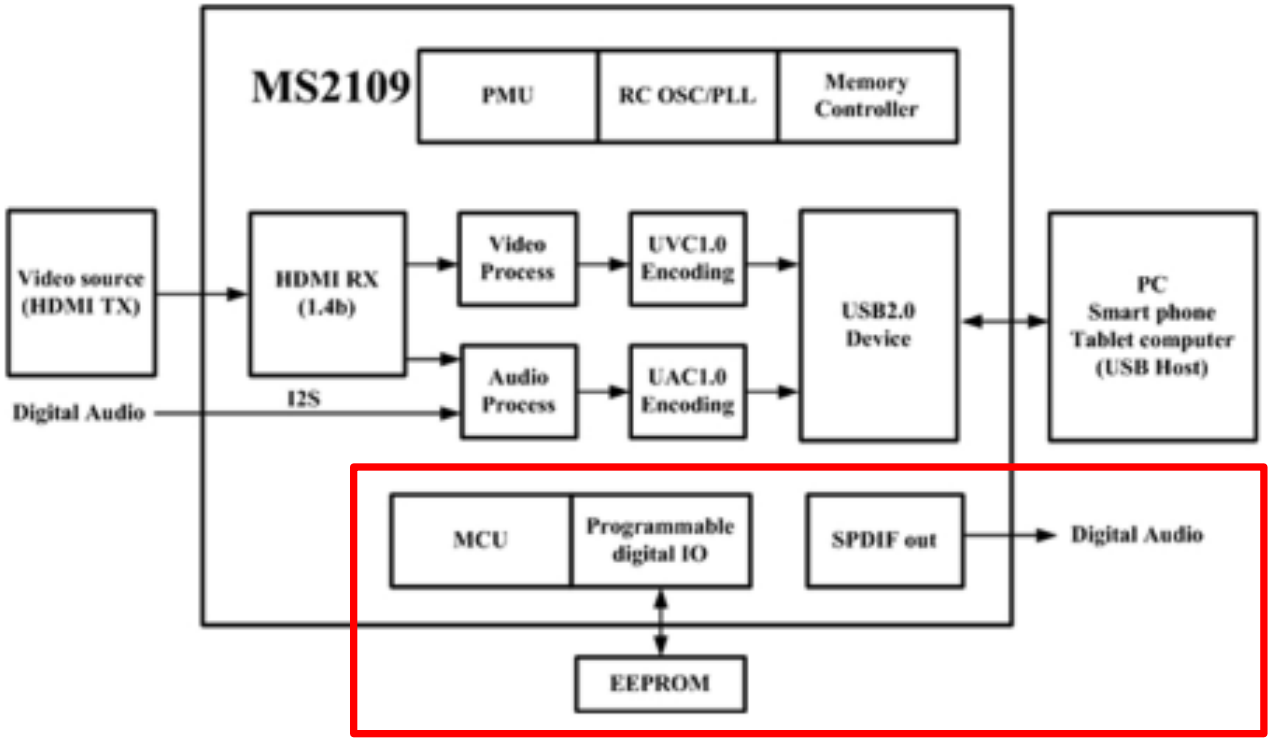
Données réinscriptibles
Elle stocke les paramètres des flux vidéos convertis par le micro contrôleur durant la période de diffusion, notamment, la qualité (720 ou 1080 par exemple), le rafraîchissement (30MHz, 60MHz etc).

Analyse de l'adaptateur HDMI - USB

Pas d'interaction avec les extrémités du convertisseur.

Function Block Diagram

Sens unidirectionnel du flux de l'HDMi vers l'USB



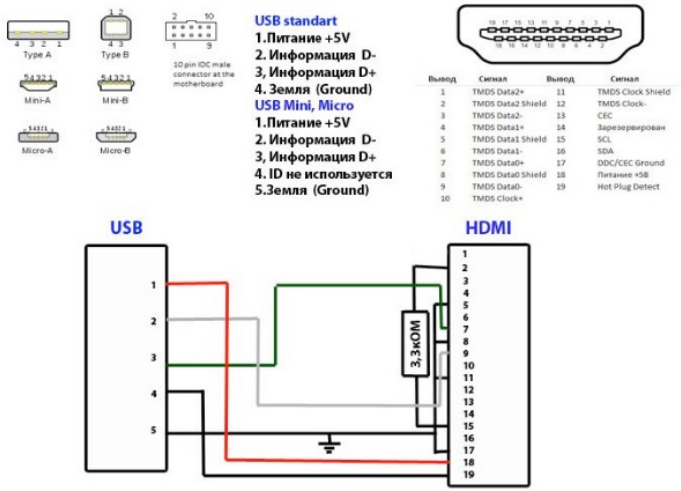
Utiliser les faiblesses de l'HDMI pour détourner les fonctions de l'adaptateur

EDID:
Dans le cas d'un pc portable, l'écran ne récupère pas ces informations car elles sont codées en dur au niveau hardware.
On peut modifier l'EDID depuis le pc portable, mais pas via la connexion HDMI.

- Le convertisseur ne permet pas depuis l'interface USB d'interagir dans ce sens avec l'HDMI

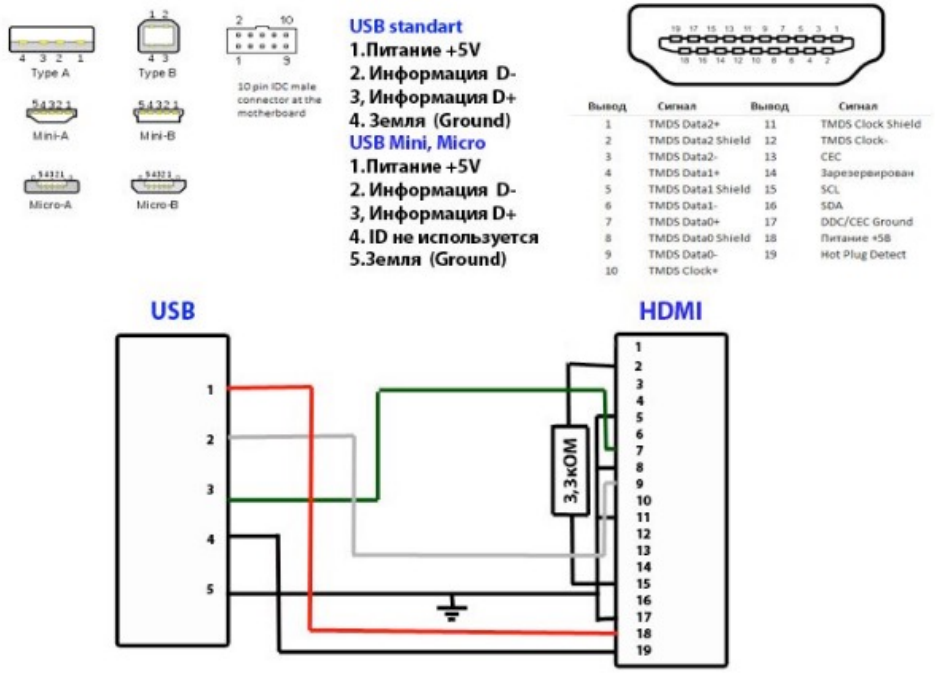
Utiliser les faiblesses de l'HDMI pour détourner les fonctions de l'adaptateur

CEC:
En analysant les schémas d'interconnexion entre USB et HDM, nous avons pu constater que le bus 13 du CEC n'est pas relié vers l'interface USB



Utiliser les faiblesses de l'HDMI pour détourner les fonctions de l'adaptateur

HEAC:
Cette fonctionnalité, qui représente un vecteur d'attaque colossal sur une architecture classique,
n'est pas présente non plus dans le convertisseur HDMI – USB (voir schéma précédent), pour les mêmes raisons que le CEC.
Le bus 14 n'est pas relié, et le bus 13, qui sert à initier HEAC n'est lui aussi pas relié.
Les vecteurs traditionnels d'attaques qu'une connexion HDMI permet ne semblent pas ici être pertinents.

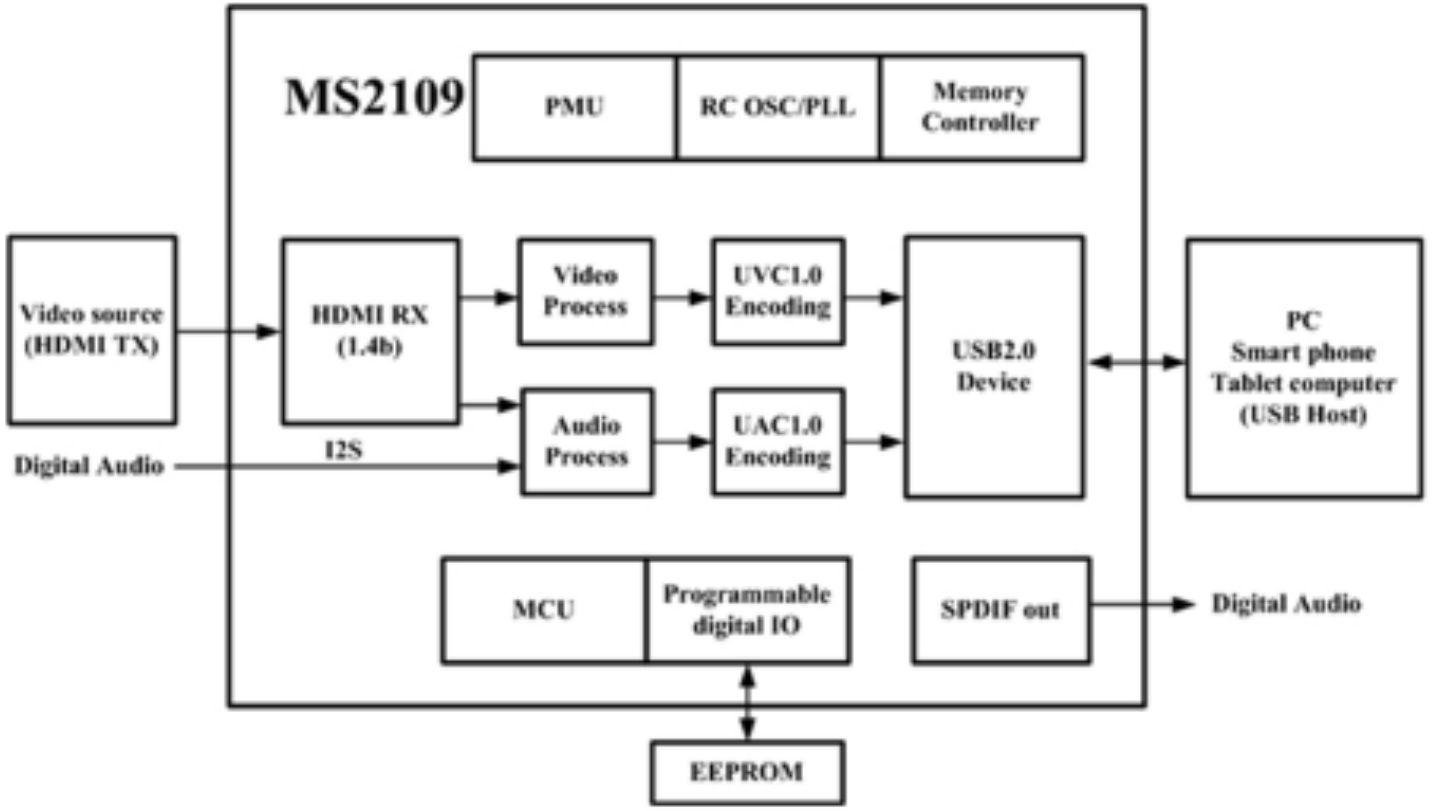


- Du coup? Vulnérable ?

Et du coup on fait quoi?

Attaques physiques

Function Block Diagram



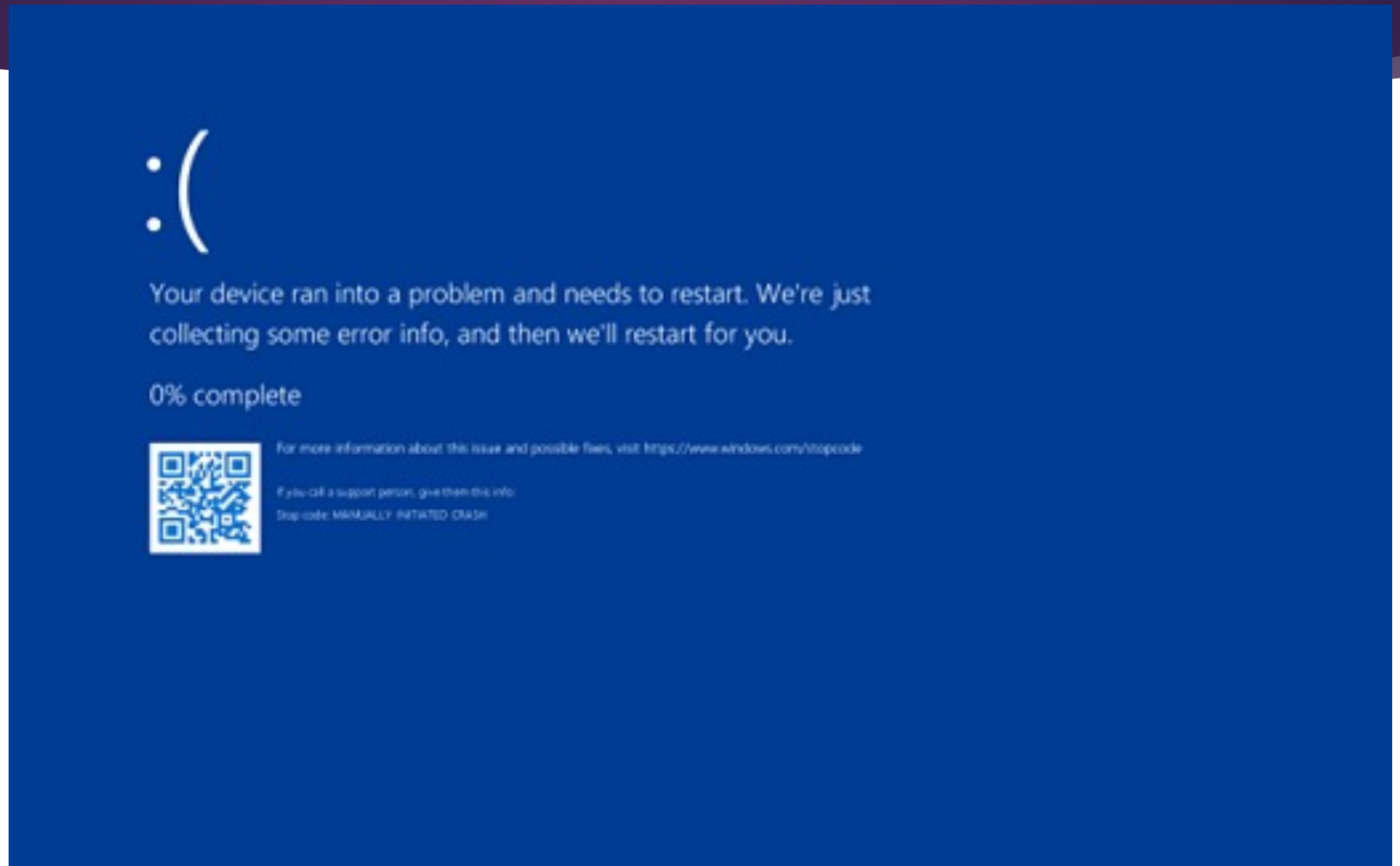
Reflash le firmware

```c
void vulnerable_function(char *input) {
    char buffer[64];  // Buffer de 64 caractères
    strcpy(buffer, input);  // Copie de l'input dans le buffer sans vérifica
}
```

```
Initialising...
Detecting device... Done.
Checking firmware... Done.
Erasing old firmware... Done.
Writing new firmware... Done.
Verifying new firmware... Done.

Firmware reflashed successfully.
```

Reflash le firmware



Conclusion

Attaques HDMI Classiques :

Les attaques classiques HDMI ne fonctionnent pas.

Attaques Software :

Les attaques logicielles visant l'USB ne fonctionnent pas.

Attaques Hardware :

Les attaques matérielles fonctionnent.