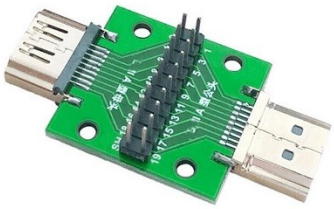
Pare-feux HDMI : signaux, protocoles, vulnérabilités

NOMS :	Date :


Objectifs :

- Lister les signaux véhiculés par une liaison HDMI, et évaluer leur niveau de vulnérabilité.
- Installer les librairies nécessaires à la mise en œuvre des bus I2C et HDMI-CEC.
- Capturer et analyser les bus les plus sensibles en mettant en œuvre un analyseur logique disposant d'interpréteurs adaptés.

Pôles d'activités / Compétences :

Pôles d'activités	Blocs de compétences

		C04 ANALYSER	C06 VALIDER
Étude et conception de produits électroniques	E2 : Tests et essais	X	X

Connaissances associées :

− Circuits : microcontrôleurs, mémoires
− Réseaux locaux industriels et bus de carte : I²C
− Appareils de mesures : analyseur logique
− Utilisation de librairies logicielles

Moyens :

- Ordinateur disposant des logiciels VNC Viewer, Scanastudio (Ikalogic) et/ou Logic2 (Saleae) et/ou WaveForms (AnalogDiscovery 2).WinSCP si on veut récupérer les fichiers Rpi sans clef USB.
- Analyseurs Ikalogic (type SQ) et/ou Saleae et/ou AnalogDiscovery.
- Nano ordinateur Raspberry Pi 3 ou 4 ; avec connectique HDMI adaptée, et liaison internet (Wi-Fi ou filaire).
- Carte de capture des signaux HDMI (aussi appelée HDMI breakout).
- Appareils disposant d'une liaison HDMI de type : Téléviseur (compatible HDMI-CEC), écran d'ordinateur, vidéo projecteur, ou écran pour affichage dynamique.
- Apparels de mesures classiques : voltmètre, ...

Conditions :

- Travail en binôme.
- Durée : 3H
- Compte rendu remis à la fin de la séance.

Prérequis :

- Avoir effectué la partie 1 : exposé de la problèmatique.
- Avoir déjà utilisé un analyseur logique.
- Notions sur : le bus I2C, les différents types de mémoires, les microcontrôleurs, checksum et crc.

Pare-feux HDMI : signaux, protocoles, vulnérabilités

Tous les documents nécessaires figurent sur le site Pare-feux HDMI

Préambule

Les 2 ressources mentionnées ci-dessous et utilisées dans la partie 1 sont également nécessaires dans cette partie 2 :

- article « Des pare-feux pour le HDMI » extrait du magazine MISC N°127,
- vidéo du symposium SSTIC 2011 portant sur le Pare-Feu HDMI.

Dans les activités qui suivent vous allez être amené à analyser des trames qui ont été capturées sur différents appareils. Il faut pour cela que les logiciels permettant de lire ces captures soient installés sur votre PC. Si ce n'est pas déjà le cas le lien de téléchargement de ces logiciels figure sur le site.

Vous allez aussi être amené à effectuer des captures de trames, bien identifier les broches concernées sur le breakout HDMI et éviter tout court circuit lors de la mise en place des sondes de l'analyseur logique.

I. HDMI : flux de données les plus sensibles, et détection de connexion

1. Prendre connaissance de la vidéo « Pare-feux HDMI : EDID, Bus I2C et HDMI-CEC » en ayant à l'esprit que s'y trouvent une bonne partie des réponses aux questions qui suivent, et qu'y sont illustrées des mises en œuvre que vous aurez vous-mêmes à effectuer.

2. Rappeler quels sont les 2 bus/protocoles qui présentent une surface d'attaque en matière de cybersécurité.

   → Bus I²C **→ Bus HDMI-CEC**

3. Lorsqu'on connecte un équipement "source" *(ordinateur, lecteur DVD, Raspberry Pi, ...)* sur un équipement "puits" *(téléviseur, écran, vidéoprojecteur, ...)* quel est le signal du connecteur HDMI qui informe immédiatement l'équipement "source" qu'un équipement "puits" vient d'être raccordé ? Quel est le niveau d'activation de ce signal ?

   → Signal HPD : Hot Plug Detect **→ actif à l'état haut pour signaler la présence d'un appareil.**

4. A partir du matériel mis à votre disposition, proposer une mesure simple permettant de vérifier votre réponse précédente. Puis la mettre en œuvre après validation par l'enseignant.

   → Intercaler un breakout HDMI entre la source et le puits, quels qu'ils soient, et disposer un voltmètre entre la broche HPD (broche 19) et le GND (broches 20, 2, 5, 8, 11). Cette broche passe à l'état haut (5V) lors de la connexion. Si la référence est la broche 17, la tension n'est que de ≈1,9V.

II. Bus I²C et EDID

5. Que veut dire l'acronyme EDID ? Quels types d'informations contiennent ces données ? Sur quel bus standard ces données sont-elles accessibles ? Dans quel type de composant électronique l'EDID est-il stocké ? Exprimer les valeurs min et max du volume de ces données, exprimé en Byte/KB ou octets/Ko.

   → EDID : Extended Display Indication Data
   → Ces données contiennent des informations sur l'appareil connecté : fabricant, date de

fabrication, différents formats d'affichage compatibles, etc...
→ Le bus I2C
→ Stocké dans une EEPROM (parfois dans un microcontrôleur).
→ 128 octets à 32Ko / 128 Byte à 32KB

Bon nombre de TV de marques différentes sont équipées des mêmes cartes électroniques, aussi appelée châssis (lien).

6. La documentation des châssis Philips TPM14.2E LA est consultable sur le site. Identifier dans cette documentation le composant qui contient l'EDID, en explicitant la méthode de recherche. Donner la référence de ce composant dans la documentation. Quelle est la référence fabricant de ce composant ? Quelle est sa capacité mémoire exprimée en octets et Byte ? Cette mémoire, telle qu'elle est câblée, est-elle éventuellement réinscriptible ?

   → U712 → Recherche par mot clef EDID
   → M24C02-WDW6P
   → 256 octets = 256 Bytes
   → Elle est réinscriptible par l'intermédiaire de la broche EDID-WC du microcontrôleur

7. La documentation des châssis Philips LC7.5E LA est consultable sur le site. Parmi les différentes mémoires présentes sur ces châssis, identifier, en explicitant la méthode de recherche, celle qui est la plus susceptible de contenir l'EDID. Donner son item *(référence qui lui est donnée dans la documentation)*. Quelle est la référence fabricant de ce composant ? Quelle est sa capacité mémoire en Kbit et KB ? Cette mémoire, telle qu'elle est câblée, est-elle éventuellement réinscriptible ?

   → 7H03 → recherche par 24C, la référence est accompagnée du commentaire I2C ADDRESS : A0
   → M24C64-WMN6
   → 64Kbit = 8 KBytes
   → Elle est réinscriptible par l'intermédiaire de la broche "user_EEPROM_WP"

8. Concernant les 2 pare-feux proposés, et la protection de l'EDID et du circuit qui le contient, quelle est la stratégie commune retenue ?

   → Les équipements de type "source" ne doivent pas avoir un accès direct à l'EEPROM et son contenu, donc une copie protégée en écriture est stockée dans le pare-feu et c'est ce circuit qui répond à la place de l'équipement "puits" lors de la connexion.

9. Préciser les 2 différences dans le stockage de l'EDID entre les 2 versions de pare-feux.

   → Version 1 du pare-feu : l'EDID est stocké dans une mémoire EEPROM. Version 2 : l'EDID est stocké dans l'EEPROM d'un microcontrôleur.

   → Version 1 : la récupération de l'EDID original se fait sur un ordinateur (ou Rpi) par l'intermédiaire d'un logiciel spécifique (sous Linux), et le fichier .bin obtenu permet de programmer l'EEPROM. Version 2 : le microcontrôleur récupère et mémorise lui-même l'EDID dans sa mémoire interne.

   Faire constater

10. Sur votre banc de travail, raccorder un Raspberry Pi à l'écran ou au téléviseur mis à votre disposition, en intercalant un breakout HDMI. Au démarrage du Raspberry Pi son bureau doit apparaître sur l'écran ou le téléviseur. Si l'équipement dispose de plusieurs connecteurs HDMI, il

faut sélectionner le bon connecteur par l'intermédiaire d'une télécommande ou des touches de l'équipement. Indiquer ci-dessous la marque et le modèle de l'équipement mis à votre disposition.

→ **Téléviseur Samsung lycée**

11. Sur le Rpi utiliser la commande permettant de détecter les circuits présents sur le bus I²C. Indiquer la commande utilisée et les adresses des circuits détectés.

→ **i2cdetect -y 2** → **Adresses 0x3a et 0x50**

12. Parmi ces adresses qu'elle est celle qui correspond à la mémoire qui contient l'EDID ? → **0x50**

13. Installer sur le Rpi la librairie qui permet de récupérer l'EDID de l'équipement.

14. Effectuer une lecture de l'EDID. Sauvegarder l'intégralité de cette lecture (EDID + décodage) dans un fichier .txt ayant votre nom et le modèle de l'équipement *(exemple « LinusTorvalds_DellSE2216H.txt »)*.

15. Quel est la chaîne de caractères du paramètre « Display Product Name » de l'équipement ?

→ **Réponse en fonction de l'équipement**

16. Sauvegarder uniquement l'EDID *(sans décodage)* dans un fichier .bin *(exemple « LinusTorvalds_DellSE2216H.bin »)*. Ces deux fichiers seront à fournir avec votre compte-rendu.

17. Le fichier .bin obtenu contient combien d'octets ? →

18. Rappeler ce qu'est un checksum et quel est son rôle. Quelle est la valeur du checksum de l'EDID que vous avez récupéré ?

→ **Somme de contrôle effectuée à partir des octets transmis, permettant de vérifier qu'il n'y a pas eu d'erreur lors de la transmission**

→ **Réponse en fonction de l'équipement**

19. Utiliser une application en ligne, par exemple celle-ci, pour vérifier la valeur du checksum obtenu, en faisant un copier/coller directement sur le site. Expliciter la méthode de calcul de cet octet.

→ **CheckSum8 2s Complement = complément à 2 de la somme de tous les octets modulo 8 bits**

20. Sur votre PC mettre en œuvre un analyseur logique, le configurer avec un interpréteur de trame I²C, puis capturer la trame de transmission de l'EDID. Sauvegarder cette capture. Identifier dans cette trame le « Display Product Name » et compare à la valeur indiquée précédemment.

→ **Réponse en fonction de l'équipement**

Faire constater

21. Une trame réalisée avec le logiciel ScanaStudio est téléchargeable sur le site. Ouvrir ce fichier sur votre PC. Décoder les champs « Manufacturer ID », « Manufacturer Product Code » ainsi que « La semaine et l'année de fabrication de l'équipement », exposer le calcul dans les 3 cas.

→ **IVM = Iiyama North America**

→ **24902**

→ **40ème semaine de 2020**

22. Toujours à partir de cette capture, déterminer la vitesse du bus I2C.

→ **100KHz**

Faire constater

III. Bus et protocole CEC

23. Rappeler en quelques mots les possibilités offertes par le bus CEC et son protocole.

→ **Permet de piloter plusieurs appareils connectés en liaison HDMI à partir d'une seule télécommande.**

24. Selon les fabricants la dénomination donnée à ce bus n'est pas la même. Indiquer cette dénomination pour les fabricants qui suivent.

→ Philips : **EasyLink** → LG : **SimpLink**
→ Samsung : **Anynet+** → Hitachi : **HDMI-CEC**

25. Le bus CEC nécessite combien de liaisons électriques ?

→ **2 liaisons : le signal CEC et le GND**

Vous avez à votre disposition un Raspberry Pi, un breakout HDMI, un téléviseur compatible avec le protocole CEC et un ordinateur disposant d'un ou de plusieurs analyseurs logiques *(de marques différentes)*.

26. Installer sur le Raspberry Pi mis à votre disposition la librairie permettant de communiquer sur le bus CEC.

27. A partir de cette librairie mettre successivement l'écran en mode « STANDBY » puis en mode « ON ». Utiliser un analyseur logique pour capturer la trame CEC lors de l'activation du mode ON. Identifier cette commande *(opcode correspondant)* dans la trame et l'indiquer ci-dessous. Sauvegarder cette capture pour une éventuelle utilisation ultérieure.

→ **Opcode 0x04 = <Image View On> = sortie du mode veille**

Faire constater

La commande suivante : **echo "ven 0" | cec-client -s -d 1** permet de récupérer le qui caractérise le fabricant.

Une capture de la trame CEC lors de cette commande vers un « Téléviseur 1 » avec le logiciel Logic2 est téléchargeable depuis le site.

28. Dans cette trame la source étant le téléviseur (0x0 = TV) et le destinataire une diffusion (0xF = Broadcast), identifier dans la trame les 3 octets émis par le téléviseur en tant que réponse à la demande "vendor ID"

    → **00903E**

29. Recopier ces 3 octets sur cette page. En déduire ce qu'ils caractérisent.

    → **Ce sont les 3 premiers octets d'une adresse MAC caractérisant le fabricant Philips**

30. Une autre capture de cette commande adressée à un « Téléviseur 2 » est également téléchargeable sur le site. En suivant la même démarche que précédemment identifier les 3 octets du "vendor ID" du téléviseur puis trouver la marque de l'appareil.

    → **00 00 F0** → **Samsung**

31. Toujours à partir des informations contenues dans cette capture, trouver la vitesse de transmission du bus CEC, et vérifier si cette valeur est conforme à la norme.

    → **Capture : 415Hz ; d'après wikipédia : 417Hz ; la valeur est donc conforme**