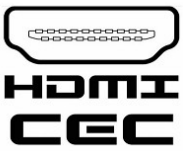
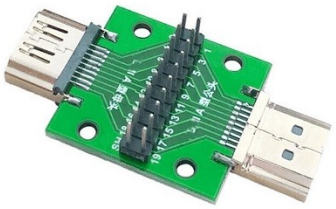
Pare-feux HDMI : signaux, protocoles, vulnérabilités

NOM :	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.

Compétence abordée	Critère d'évaluation de la compétence
C04 : Analyser une structure matérielle et logicielle	Les spécifications du cahier des charges sont extraites La fonction des structures et des composants est critiquée

Compétence abordée	Critère d'évaluation de la compétence
C06 Valider une structure matérielle et logicielle	Les procédures de test sont mises en œuvre

Compétence abordée	Critère d'évaluation de la compétence
C09 Installer un système électronique ou informatique	Les éléments du système sont installés et raccordés, les logiciels sont installés

Connaissances associées :

- Circuits : microcontrôleur, mémoires
- Réseaux locaux industriels et bus de carte : I²C, CEC
- Technologie de raccordement (filaire, ..)
- Appareils de mesures (analyseur logique)
- Analyse et caractérisation temporelle et fréquentielle des signaux
- Utilisation de librairies logicielles

Moyens :

- Ordinateur disposant des logiciels VNC Viewer, Scanastudio (Ikalogic) et/ou Logic2 (Saleae) et/ou WaveForms (AnalogDiscovery 2).
- 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.
- Appareils de mesures classiques : voltmètre, ...

Conditions :

- Travail en binôme.
- Durée maximale : 2 x4H
- Compte rendu remis à la fin de la séance.

Prérequis :

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

Pare-feux HDMI : signaux, protocoles, vulnérabilités

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

A noter : 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 : fabriquer et tester la version à microcontrôleur» en ayant à l'esprit que s'y trouvent une bonne partie des réponses aux questions qui suivent, ainsi que l'illustration des procédures à suivre pour la fabrication et qu'y sont illustrées des mises en œuvre que vous aurez vous-mêmes à effectuer. *La vidéo est chapitrée mais en cas de besoin, dans le déroulé du questionnaire ce logo* ▶ *constitue un lien qui cale la vidéo sur la partie abordée*.

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

   → →

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 ?

   → →

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.

   →

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.

→
→

→
→
→

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

→

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

→

→

Faire constater

8. 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.

→

9. 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.

→ →

10. Parmi ces adresses qu'elle est celle qui correspond à la mémoire qui contient l'EDID ? →

Bon nombre de TV de marques différentes ont les mêmes cartes à l'intérieur, aussi appelée châssis (lien).

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

→

→
→
→

12. La documentation des châssis Philips LC7.5E LA est consultable sur le site. Parmi les différentes mémoires présentes sur ces châssis, identifier celle qui est la plus susceptible de contenir l'EDID, expliciter la méthode de recherche et justifier ce choix, donner son item *(référence dans la documentation)*. Quelle est la référence fabricant de ce composant ? Quelle est sa capacité mémoire en Kbit et Kbyte ? Cette mémoire est-elle éventuellement réinscriptible ?

→
→
→
→

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

→

16. Sauvegarder uniquement l'EDID *(sans décodage)* dans un fichier .bin ayant votre nom et le modèle de l'équipement *(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 ?

→

→

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.

→

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 comparer à la valeur indiquée précédemment.

→

Faire constater

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

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.

    →

    →

    →

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

    →

Faire constater

III. Bus et protocole CEC

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

    →

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

    → Philips :
    → LG :
    → Samsung :
    → Hitachi :

25. Le bus CEC nécessite combien de liaisons électriques ?

    →

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.

→

Faire constater

La commande suivante : **echo "ven 0" | cec-client -s -d 1** permet de récupérer le "vendor ID" 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"

    →

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

    →

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.

    → →

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

    →

Faire constater