



Pare-Feux HDMI : analyse, validation, réalisation et installation.

BTS
CIEL option Électronique et Réseau

Auteur (s)

Hortolland Christian, lycée Alphonse Benoit à l'Isle sur la Sorgue, académie d'Aix-Marseille, agrégé en électronique.

Description

Ce module de formation m'a été inspiré par un article du N°127 du magazine MISC ([lien](#)) coécrit par 2 deux chercheurs en sécurité informatique de l'ANSSI et un ingénieur consultant en sécurité embarquée et mobile.

Cet article porte sur un exposé ayant eu lieu lors d'un symposium du SSTIC ([lien](#)) exposant les failles de sécurité informatique possibles lors de l'utilisation d'un câble HDMI, failles qui peuvent venir de l'un des différents bus qui parcourent ce type de câble.

L'article présente 2 cartes électroniques permettant de protéger le système contre ce type de vulnérabilité.

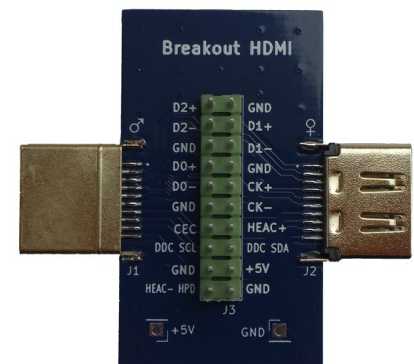
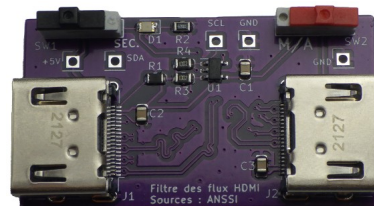
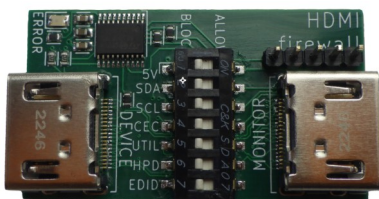
La première solution reposant sur l'utilisation d'une mémoire morte EEPROM a fait l'objet d'une réalisation dont les documents de fabrication (*sous-traitée par l'ANSSI à une entreprise tiers*) n'ont pas été mis en partage. Ultérieurement une seconde réalisation, reposant sur un microcontrôleur, et proposant un filtrage des bus un peu plus sélectif (*moins exclusif*) a été développée, cette solution est open source au niveau matériel ([lien 1](#)), et logiciel ([lien 2](#)).

Intention pédagogique

Les exploitations possibles, avec des étudiants de BTS CIEL ER, sont nombreuses.

- Tout d'abord exposer la problématique de cybersécurité mise en évidence par l'ANSSI, et effectuer des captures sur quelques-uns des bus véhiculés par un câble HDMI, en utilisant une petite carte de test que l'on trouve sur internet. Cela permet d'amener l'étudiant à installer quelques bibliothèques sous Linux, et à mettre en œuvre un analyseur logique avec interpréteurs de trames pour analyser certains des échanges (bus I2C et CEC, par exemple).
- Ensuite il est intéressant de récupérer les documents de fabrication de la seconde version du pare-feu, pour les analyser aussi bien au niveau du schéma structurel que du routage. Pour respecter des contraintes liées à la CEM le circuit imprimé a été réalisé en 4 couches. Le fait d'identifier les composants à commander pour effectuer la fabrication est également intéressant. Le projet a été développé sous KiCAD, logiciel gratuit mais aux performances tout à fait comparables à celles de logiciels professionnels. Les collègues qui ne travaillent pas avec ce logiciel pourront tout de même récupérer les fichiers Gerber pour effectuer les étapes suivantes, qui consistent à faire fabriquer les PCB, puis à les câbler avec les étudiants, programmer le microcontrôleur du pare-feu et vérifier le bon fonctionnement de la structure en s'assurant que certains bus ne passent plus que sélectivement.

- L'étape suivante consiste, en s'inspirant de la réalisation précédente, à amener les étudiants en les guidant pas à pas, à concevoir la première version du pare-feu, dont les documents n'ont pas été partagés. Cela amène entre autres, avec KiCAD, ou un autre logiciel, à router une carte sur 4 couches (2 plans de masse internes), et à s'initier au routage de paires différentielles. Ce qui aboutira au câblage de la carte (*à partir du routage des étudiants, ou de celui de l'enseignant avec une solution viable*), à sa programmation et aux essais de validation.
- Une dernière étape, consiste pour l'étudiant à concevoir une petite carte de test d'une liaison HDMI, du même type que celle utilisée dans la première phase, mais mieux adaptée au repérage des signaux des différents bus lors de la capture des trames, et mettant également en œuvre le routage de paires différentielles. Le travail sera nettement plus simple que dans la version précédente mais l'étudiant devra montrer son niveau d'autonomie.



J'ai pu vérifier le bon fonctionnement des solutions proposées pour les 2 pare-feux. De très petites adaptations matérielles et logicielles sont nécessaires par rapport aux documents mis en ligne, ce qui présente aussi un certain intérêt.

Les établissements qui souhaitent réaliser leurs PCB en utilisant une CNC pourront faire les 2 dernières réalisations en version 2 couches, ce qui devrait également fonctionner.

Les fichiers Gerber de ces 2 dernières réalisations pourront être fournis aux collègues qui seraient uniquement intéressés par le câblage et la mise en œuvre.

L'investissement est très raisonnable.

Les échanges pour la configuration/programmation des cartes pare-feux doivent se faire entre un PC sous Linux ou un Raspberry Pi (*j'ai fait mes essais sur Rpi3*) et un écran, ou un téléviseur, ou un vidéoprojecteur avec une connectique HDMI. Si on dispose d'un téléviseur compatible HDMI-CEC c'est l'idéal.

Il faut également disposer d'un analyseur logique, plusieurs modèles proposent les interpréteurs de trames nécessaires (*I2C et HDMI-CEC*).



Les cartes pourront éventuellement servir ensuite en tant qu'auto-équipement.

Pré-requis

- Avoir déjà pratiqué une saisie de schéma et un routage sur un ou des exemples simples.
- Connaissances minimales sur l'environnement Linux.
- Connaissances minimales de programmation en langage C/C++.
- Si possible avoir déjà utilisé un analyseur logique.

Pôles d'activités / Compétences

Pôles d'activités		Blocs de compétences			
		C04 ANALYSER	C06 VALIDER	C07 RÉALISER	C09 INSTALLER
<i>Étude et conception de produits électroniques</i>	E1 : Étude et conception de produits électroniques	×	×	×	
	E2 : Tests et essais	×	×		
<i>Réalisation et maintenance de produits électroniques</i>	E3 : Production et assemblage d'ensembles électroniques			×	×
	E4 : Intégration matérielle et logicielle	×		×	×

Connaissances associées :

- Gestion des commandes
- Circuits : microcontrôleurs, mémoires
- Réseaux locaux industriels et bus de carte : I²C
- Programmation en langage C
- Appareils de mesures : analyseur logique
- Technologies de boîtiers de composants : CMS, traversant, connectiques
- Technologies de fabrication d'un PCB
- Procédés de pose et brasure
- Procédés de prototypage
- Utilisation de bibliothèques logicielles



Modalités

Période : soit au second semestre de première année, soit au premier semestre de la deuxième année.

Volume horaire indiqué de façon très approximative, je vais prochainement effectuer ces activités avec mes propres élèves (SN2 EC), ce qui me donnera une idée plus précise.

Période	Première année <input type="checkbox"/>		Deuxième année <input type="checkbox"/>	
	S1	S2	S1	S2
Modalités		Soit	Soit	
Volume horaire		~ 30H	~ 30H	

Ressources

Supports de cours	Site en ligne (à l'image de celui réalisé pour une précédente production : lien)	Tous les sujets de travaux dirigés et pratiques (<i>format .pdf téléchargeable</i>), les documentations, liens utiles, librairies, etc... seront accessibles en ligne. Tutoriels vidéos d'accompagnement pour chaque activité (lien vers celui de la mise en situation), pour faciliter l'autonomie des étudiants.
Évaluations	Les 3 premières activités pourront faire l'objet d'une évaluation en cours d'apprentissage.	La dernière activité pourra être davantage vue comme une évaluation sommative. Une évaluation finale écrite pourra être effectuée en fin de parcours, portant sur les connaissances théoriques et pratiques abordées.
Sujets TD/TP	4 sujets de TD/TP	Sujet de TD et de mise en pratique pour chaque activité
Doc. de référence	Site en ligne	Toutes les documentations, liens utiles, librairies ... seront accessibles en ligne



Supports

Matériels :

Téléviseur ou écran dynamique compatible HDMI-CEC, sinon écran d'ordinateur ou vidéoprojecteur.

Raspberry Pi.

PC équipé :

- d'un analyseur logique avec interpréteur I2C et CEC (*Analog Discovery, Ikalogic, Saleae, ...*)
- de VNC Viewer

Matériel de brasage.

ST-Link V2 Mini débogueur/programmeur pour STM8

Carte de test/breakout pour liaison HDMI

Logiciels :

- logiciel de saisie de schéma et de routage (*KiCAD si possible mais non obligatoire*).
- bibliothèques à ajouter en ligne sous Linux

Partenaires

Le N°127 du magazine MISC sera nécessaire, charge à chaque établissement de se le procurer soit sous forme papier, soit sous forme de liseuse HTML.

Je ne mettrai pas dans les ressources de version scannée de l'article pour des raisons de respect des droits d'auteurs. Sauf si des droits de publication sont négociés, mais ce n'est pas de mon ressort.