Risques associés aux signaux parasites compromettants : le cas des câbles DVI et HDMI

Pierre-Michel Ricordel et Emmanuel Duponchelle
prenom.nom@ssi.gouv.fr

Laboratoire Sécurité des technologies Sans Fil
Agence Nationale de la Sécurité des Systèmes d'Information

1 Contexte

Le mot-clef TEMPEST désigne l'ensemble des mesures de protection mises en place afin de protéger des équipements traitant des informations sensibles contre l'interception des signaux électromagnétiques qu'ils seraient susceptibles d'émettre accidentellement.

Selon la légende, la découverte de ces signaux parasites compromettants (SPC) remonte à la seconde guerre mondiale, lorsque des ingénieurs de Bell Telephone découvrent avec stupeur qu'ils parviennent à intercepter les messages clairs traités par le centre cryptographique des Signal Corps, à l'aide des oscilloscopes de leur laboratoire situé de l'autre côté de la rue, à 25 mètres de là [1]. À cette époque les systèmes interceptés étaient des télétypes électromécaniques.

Cette menace a rapidement été prise au sérieux par les grandes puissances, notamment les États-Unis, et par extension les pays de l'OTAN, pour lesquels cette menace est associée au nom de code TEMPEST. Pour contrer cette menace, un cadre normatif a été mis en place, couvrant le blindage des équipements, la protection des sites et les méthodes de mesures. Le secret couvrant ces normes, qui traitent de phénomènes complexes et difficiles à expliquer, et dont les effets pourraient presque paraître surnaturels (on n'est pas loin de la clairvoyance), ont rendu ce domaine mystérieux pour le grand public. Quelques rares chercheurs ont publié des travaux sur le domaine, notamment Wim Van Eck [2], popularisé par l'auteur de science-fiction Neal Stephenson [3], ou Markus Kuhn de l'université de Cambridge [4]. Plus récemment, Martin Marinov, également de l'université de Cambridge [5], a publié TempestSDR, le premier outil OpenSource permettant de reconstituer en temps réel l'image vidéo d'un écran à partir de signaux parasites [6].

2 Les normes TEMPEST en France

L'ANSSI édite une démarche de sécurisation destinée à protéger le risque de compromission d'information par captation de SPC. La mise en œuvre de l'instruction interministérielle n°300 [7] est recommandée pour protéger les informations sensibles des entreprises par exemple. Cependant son application est obligatoire pour le traitement d'information classifiée de défense.

Plusieurs solutions sont proposées pour protéger la confidentialité des informations traitées :

- l'installation des systèmes sensibles dans les pièces les moins exposées au risque, c'est à dire les plus éloignées des zones publiques et des murs et planchers mitoyens ;
- la prise en compte de l'atténuation que la structure des bâtiments apporte aux signaux radiofréquences. Il s'agit du principe du zonage TEMPEST des locaux ;
- Le choix de technologies limitant les risques d'interception, tel que l'emploi de fibre optique ou l'utilisation d'équipements spécialement conçus pour limiter au maximum le niveau des SPC produits par l'ordinateur. On parle alors de « matériel certifié au plan TEMPEST ».

En cas d'impossibilité d'appliquer la démarche de sécurisation proposée, l'emploi d'une cage de Faraday peut devenir une solution alternative.

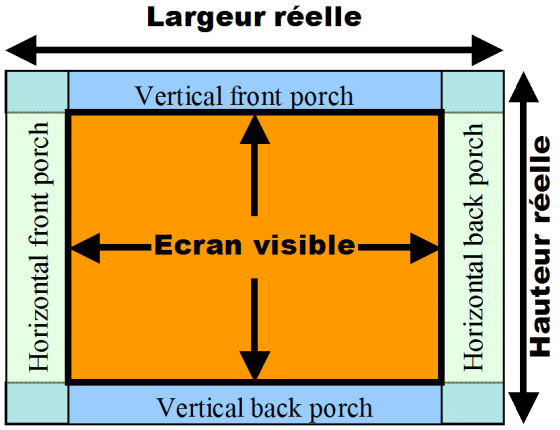
3 Évolution de la menace : le cas du signal vidéo

La menace est ancienne, mais elle s'applique toujours aux systèmes actuels. Si beaucoup de technologies considérées à risque sont devenues obsolètes, comme les téléimprimeurs, les écrans cathodiques ou les claviers PS/2, d'autres technologies les ont remplacées, et sont elles aussi des sources potentielles de signaux compromettants. Les signaux lents et de grande amplitude sont devenus des signaux différentiels ultra rapides. Mais si les grandeurs physiques et les modes de fuite ont changé, la menace existe toujours.

Prenons à titre d'exemple les signaux passant dans le câble vidéo d'un ordinateur. Autrefois analogique (norme VGA), le signal vidéo est devenu numérique (norme DVI, ou norme HDMI, cette dernière véhiculant principalement des signaux DVI).

3.1 Les signaux VGA

Dans le cas du signal VGA, le signal vidéo est transmis sur trois câbles coaxiaux (un par couleur élémentaire : rouge, vert, bleu). Pour chaque couleur élémentaire, l'intensité d'un pixel est codée par une tension comprise entre 0 Volt et 0,7 Volt, dont la valeur dépend linéairement de l'intensité. Les pixels sont transmis séquentiellement, ligne par ligne, de gauche à droite et de haut en bas, l'ensemble formant une trame. Les trames sont transmises continuellement, à la fréquence dite de rafraîchissement de l'écran (ou fréquence trame). Généralement des marges horizontales et verticales sont réservées autour de l'image visible, afin de laisser du temps à l'électronique de contrôle de l'écran de se préparer à passer d'une ligne à l'autre, et d'une trame à l'autre.



Nous obtenons donc 3 fréquences cruciales pour l'interprétation d'un signal VGA :

- la fréquence trame, c'est-à-dire la fréquence de répétition d'une trame, généralement aux alentours de 60 Hertz ;
- la fréquence ligne, qui est le produit de la fréquence trame et du nombre de lignes d'une trame (ce nombre inclut les lignes visibles et les lignes des marges invisibles en haut et en bas), faisant généralement plusieurs dizaines de kilohertz ;
- la fréquence pixel, qui est le produit de la fréquence ligne et du nombre de pixels par ligne (ce nombre inclut les pixels visibles et les pixels des marges invisibles à gauche et à droite), faisant généralement plusieurs dizaines de mégahertz.

À titre d'exemple, pour un signal HD 1080p 60 Hz (1920x1080), le standard HDTV prévoit 280 pixels de marges horizontales et 45 pixels de marges verticales, soit un total de 2200x1125 pixels. La fréquence trame est

fixée à 60 Hertz, donc la fréquence ligne est de $60 \times 1125 = 67,5$kilohertz, et la fréquence pixel est de $67,5kHz \times 2200 = 148,5$mégahertz.

Afin d'aider l'écran à se synchroniser à ce signal, le câble VGA véhicule également des signaux de synchronisation donnant les temps de début de lignes et début de trames.

Un blindage n'étant jamais parfait, une partie de l'énergie de ces signaux va s'échapper du câble par rayonnement. Ce rayonnement est associé aux variations du signal, et non à son niveau continu. En effet, ce sont les fronts, montants ou descendants, d'un signal qui génèrent des signaux parasites, et plus ces fronts sont raides (plus le dV/dt est important), plus l'énergie rayonnée augmente.

Le signal VGA est relativement rapide, il est donc propice au rayonnement, mais la présence ou non de fronts est conditionnée au contenu de l'image, notamment aux variations brusques d'intensité lumineuse au sein d'une ligne. Ainsi sur la capture ci-dessous, on constate que seules les frontières verticales des lettres sont visibles, lorsque ces lettres présentent un fort contraste par rapport au fond.

3.2 Le raster

Le but d'un raster, comme TempestSDR, est de reconstituer l'image affichée à l'écran, à partir des signaux parasites corrélés à des signaux d'écran. En l'occurrence, il peut s'agir des signaux rayonnés par le câble VGA, qui sont détectés (démodulés en amplitude) par un récepteur à une fréquence donnée, avec une bande passante suffisamment large par rapport à la fréquence pixel. Une grande bande passante est capitale car c'est elle qui va déterminer la netteté horizontale de l'image : le rapport de la fréquence pixel sur la bande passante donne la largeur du flou, en pixels.

Le fonctionnement d'un raster est similaire à celui d'un écran : il doit restituer sur une image l'intensité du signal, en balayant de gauche à droite et de haut en bas. La seule différence est qu'il n'a pas accès aux signaux de synchronisation ligne et trame. Il doit donc reconstituer ces signaux.

Ces derniers étant réguliers, il suffit de retrouver leur fréquence et leur phase pour retrouver l'image originale. Outre l'affichage de l'image, une fonction essentielle d'un raster est donc d'assister l'opérateur à retrouver, avec une grande précision, ces fréquences ligne et trame. Une fonction importante du raster est également de pouvoir moyenner plusieurs trames successives, afin d'améliorer le rapport signal à bruit de l'image.

Il faut noter que l'image d'un raster sera toujours monochrome, les rayonnements des câbles rouge, vert et bleu s'additionnant et ne pouvant pas être différenciés au niveau de l'antenne de réception.

3.3 Les signaux DVI et HDMI

Les signaux véhiculés par les câbles DVI ou HDMI sont des signaux numériques différentiels transmis sur des paires torsadées. Le signal HDMI est identique au signal DVI. Usuellement, 4 paires sont utilisées : 3 véhiculant les couleurs rouge, vert et bleu, et la dernière véhiculant un signal d'horloge synchronisant le flux binaire. Dans les câbles DVI, trois paires supplémentaires peuvent être utilisées pour doubler le débit rouge, vert, bleu pour les très hautes résolutions. Ces paires supplémentaires n'existent pas dans les câbles HDMI.

Une particularité du signal DVI est qu'il reprend exactement les mêmes contraintes temporelles que le signal VGA : les fréquences pixel, ligne et trame ne changent pas par rapport au VGA. Ce qui change est la méthode de transmission de l'information. Ainsi, au lieu de transmettre l'intensité d'un pixel par un niveau analogique, celle-ci est transmise par l'envoi d'un code binaire de 10 bits. Ce code binaire est issu de l'algorithme TMDS encodant 8 bits dans 10 bits, qui minimise le nombre de transitions et qui équilibre le nombre de 0 et de 1 afin d'améliorer la fiabilité de la transmission. Les signaux de synchronisation ligne et trame sont encodés dans les marges du signal bleu. En HDMI, les marges vidéo sont également utilisées pour encoder de l'audio numérique.

Le signal DVI est donc un signal numérique dix fois plus rapide que le signal VGA. Ainsi pour le mode HD 1080p, avec une fréquence pixel de 148,5 MHz, les paires différentielles transmettent 1485 Mbit/s chacune. Comparativement au VGA, les fronts de tension sont beaucoup plus nombreux et plus rapides. Une autre différence est que, même si l'intensité d'une séquence de pixels ne varie pas (par exemple une ligne de couleur unie), il y aura quand même la présence de fronts binaires, et donc d'énergie pouvant être rayonnée. De plus, malgré la complexité de l'algorithme TDMS, la distribution en fréquence de l'énergie rayonnée dépend fortement de la valeur binaire transmise.

Cette dépendance, ainsi que la similitude temporelle du signal DVI au signal VGA explique pourquoi un raster fonctionne aussi bien en VGA qu'en DVI. Ainsi, à une fréquence donnée, chaque valeur de pixel 0 à 255 va générer une intensité différente (mais non proportionnelle) de parasites, qui vont permettre avec une bonne probabilité de discerner le contenu de l'écran. Il n'est pas nécessaire de multiplier la bande passante par 10 (ce qui serait coûteux et contre-productif), car l'unité d'information est toujours le pixel, et l'intensité moyenne du code TDMS de 10 bits suffit pour interpréter l'information présente à l'écran. La capture ci-dessous illustre ce phénomène. On constate par exemple que seule une partie de la photo est reconnaissable, mais elle est en inversion vidéo, alors que le texte ne l'est pas.

3.4 Les défauts de blindages DVI et HDMI

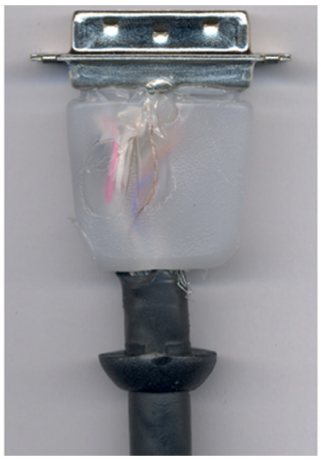
Nous avons vu que les signaux DVI sont beaucoup plus rapides que les signaux VGA, et présentent beaucoup plus de fronts raides, et donc sont très susceptibles de rayonner des signaux parasites compromettants. Le blindage de ces signaux est donc capital. Les signaux sont véhiculés dans un câble blindé contenant les paires différentielles. Généralement nous constatons que le câble proprement dit n'est pas une source de rayonnement significative, car son blindage est standardisé et répond à des normes strictes de compatibilité électromagnétique. En revanche, le raccordement du câble au connecteur DVI ou HDMI peut parfois faire défaut, notamment au niveau du raccordement de la tresse de blindage du câble avec le corps du connecteur. En effet, si cette reprise du blindage n'est pas faite de manière continue tout autour du connecteur, le blindage est inefficace et un rayonnement très intense s'échappe à ce niveau.

L'analyse par démontage de dizaines de câbles DVI et HDMI permet de dégager une tendance générale. 4 types de blindages ont été rencontrés :

– l'absence totale de blindage. Bien évidemment ce type de cordon rayonne beaucoup ;

- la présence d'un blindage partiel en feuille de cuivre, et d'un raccord de la tresse par une « queue de cochon », c'est-à-dire que la continuité électrique entre la tresse du cordon et le blindage du connecteur n'est faite que par un fil simple. Ce type de cordon rayonne beaucoup car ce type de blindage est inefficace à haute fréquence ;
- la présence d'un blindage en feuille de cuivre avec un raccord soudé à 360° de la tresse du cordon. Ce type de câble rayonne très peu ;
- la présence d'un capot acier blindé, qui pince la tresse du cordon. Ce type de capot n'a été rencontré que pour des connecteurs DVI. Ce type de câble rayonne très peu.

Les photos suivantes montrent des exemples de câbles DVI et HDMI de ces quatre types de blindages.

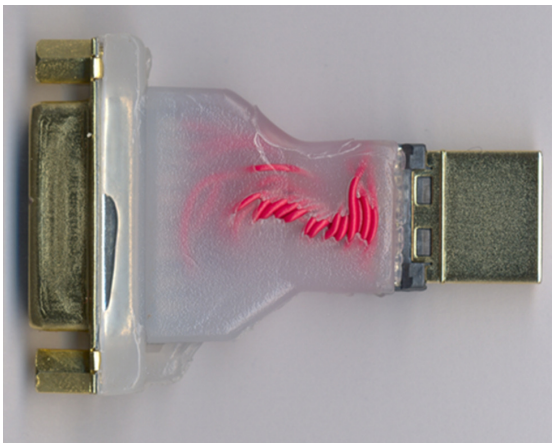



La provenance du câble conditionne très souvent sa qualité. Nous avons constaté que dans la très grande majorité des cas, les câbles de mauvaise qualité (les deux premiers types) sont des câbles achetés au détail, alors que les câbles de bonne qualité (les deux derniers types) ont été livrés avec des unités centrales ou des écrans de grands constructeurs informatiques. Notre analyse est que seuls ces derniers sont obligés de respecter des normes de compatibilité électromagnétique. Les fabricants de câbles au détail font l'économie du blindage, ou ne vérifient pas la qualité de leur fabrication. Le prix, l'aspect visuel, ou l'effort de marketing fabricant n'a généralement aucun impact sur la piètre qualité du blindage. Certains prétendent même que leur câble apporte une protection anti-virus[1] !

Les convertisseurs de type, comme l'adaptateur DVI-HDMI illustré ci-dessous, sont également concernés par ce phénomène. Un adaptateur

[1] `http://www.zdnet.com/article/this-xbox-hdmi-cable-has-anti-virus-protection/`

mal blindé peut entraîner un rayonnement très important, même s'il est raccordé à de bons câbles.



Nous estimons que le rapport des rayonnements entre un bon blindage et un mauvais blindage peut atteindre 30 dB, ce qui a pour conséquence de multiplier la distance théorique d'interception par 32. Ainsi, si avec un câble DVI correctement blindé il devient difficile de capturer son signal à plus de 1 mètre, le même résultat sera atteint à 32 mètres d'un câble DVI mal blindé.

4 La protection TEMPEST ou « le bon équipement à la bonne place »

L'**hypothèse initiale** est que l'attaquant n'a pas accès physique à la cible. La cible peut être par exemple un ordinateur utilisé pour le développement de nouveaux produits, un vidéo projecteur de la salle de réunion où se déroule des présentations stratégiques pour la direction, ou bien encore un mur d'images permettant le suivi d'une opération sensible en cours.

Le **« bon équipement »** signifie d'utiliser un équipement limitant le risque d'interception TEMPEST soit parce qu'il a été conçu en ce sens « équipement TEMPEST »[2], soit parce qu'il a été évalué au plan TEMPEST[3]. Le but de ces évaluations est de détecter des problèmes de blindages tels que ceux décrit dans cet article. De plus, il conviendra de choisir un équipement ne disposant pas d'interface radio fréquence (RF).

[2] Par exemple il existe une liste d'entreprises accréditées par l'OTAN (`https://www.ia.nato.int/niapc/tempest/certification-scheme`), et par l'UE (`https://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/information-assurance/tempest/`)

[3] On peut citer par exemple le BSI Zoning list : `https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSITL03305/TL_03305_pdf.pdf`

Si l'utilisation de technologie RF est indispensable, il conviendra alors de sécuriser correctement le lien radio.

La « **bonne place** » signifie d'installer l'équipement, ou le système, dans un environnement limitant les risques d'accès physique, de surveillance visuelle, d'interception acoustique et électromagnétique. Pour cela, la protection est généralement basée sur le principe de cloisonnement. L'accès au bureau à protéger doit être protégé physiquement. On va chercher à cloisonner visuellement ce bureau vis-à-vis de l'extérieur en fermant les rideaux par exemple. On isolera acoustiquement ce bureau vis-à-vis des bureaux ou locaux voisins. On veillera à ne pas autoriser la présence d'équipement communicant tel que des enceintes connectées ou des téléphones portables dans les locaux sensibles. De plus, on limitera au maximum la présence d'équipements électroniques non maîtrisés comme les systèmes de domotique superflus. Finalement on tentera de confiner les ondes électromagnétiques à l'intérieur du bureau à protéger.

Le confinement électromagnétique, aussi nommé **protection TEMPEST de l'infrastructure**, consiste à identifier les chemins de fuite électromagnétique afin d'apporter un durcissement à chacun d'eux si nécessaire.

Ces **chemins de fuites** sont de deux types : en rayonnement ou en conduction.

Le phénomène de **propagation par rayonnement** présente la particularité d'être prédictible. En effet, l'interception TEMPEST est facilitée lorsque l'attaquant se trouve à proximité de la cible. Le principe de précaution qui en découle consiste donc à s'éloigner, protection par la distance, ou à estimer l'atténuation des murs et plafonds, **mesure de zonage TEMPEST**. Cette mesure basée sur le principe de la double pesée consiste à établir une mesure de référence puis de la comparer à une mesure effectuée entre l'intérieur du local, où se trouve l'équipement à protéger, et l'extérieur du bâtiment, là où un attaquant pourrait s'installer.

Le phénomène de **propagation par conduction** est plus difficile à appréhender. Si l'équipement est placé à proximité d'un conducteur métallique (canalisations de chauffage central, tuyauterie d'air conditionné ou câblages électriques par exemple), aussi nommé conducteur fortuit, les signaux vont se propager le long de support et « polluer » les éléments métalliques à leur proximité. Ceci implique qu'il est difficile de prédire jusqu'à quelle distance le signal compromettant sera accessible.

Une mesure similaire au zonage TEMPEST peut être envisagée afin de quantifier l'affaiblissement des ondes électromagnétiques se propageant en conduction sur les conducteurs métalliques. Le principe sera alors de

réaliser une mesure de référence sur le conducteur à tester, puis de réaliser la mesure entre le local à protéger et les éléments métalliques accessibles par l'attaquant. Si l'atténuation mesurée est suffisante, il n'est alors pas nécessaire de recourir à l'installation d'un moyen de protection. Par contre si ce n'est pas le cas, plusieurs solutions de durcissement sont envisageables. Il s'agit soit d'éloigner l'équipement à protéger des conducteurs fortuits, soit d'effectuer une **mesure en conduction** sur le conducteur incriminé. En fonction du résultat obtenu, si nécessaire, il conviendra alors d'insérer des moyens de protection ad hoc. Ceux-ci peuvent avoir pour but de stopper la propagation des signaux en « coupant » (isolation galvanique) le support de conduction en utilisant un manchon isolant par exemple, ou de limiter leur propagation en insérant un filtre atténuant grandement le niveau des signaux compromettants. Une fois les dispositifs de protection mis en place, il conviendra d'effectuer une nouvelle mesure en conduction afin de valider leur efficacité.

En résumé, le principe de protection est donc de s'éloigner des locaux mitoyens, des tuyaux de chauffage ou de tout conducteur métallique.

Si les précautions présentées ci-dessus ne sont pas applicables, des solutions alternatives peuvent être envisagées, comme par exemple l'emploi de tissus ou peintures conductrices à appliquer sur les murs et fenêtres ou encore l'utilisation de baie informatique durcie vis-à-vis de la compatibilité électromagnétique (CEM) comme celles utilisées parfois en industrie à proximité de machines tournantes ou de robots. Dans les cas extrêmes, l'emploi d'une cage de Faraday peut se révéler être une solution pragmatique et pérenne à condition d'effectuer correctement la maintenance des ouvrants, sinon il y a risque de fuite, et donc potentiellement de compromission.

5 Conclusion

Nous montrons ici que la menace TEMPEST perdure, et que l'évolution des technologies n'y change rien, en illustrant nos propos par le signal vidéo, qui est un signal particulièrement sensible car il est à la fois riche en information et répétitif (il est retransmis 60 fois par secondes). D'autres signaux peuvent également être concernés, par exemple ceux des claviers [8], des imprimantes, etc.

La réglementation TEMPEST éditée par l'ANSSI [7] est un outil permettant de réduire les risques associés à ces menaces.

Références

1. David G. Boak. A History of U.S. Communication Security (Volumes I and II). *Lectures, National Security Agency*, P.90, 1973.
2. Wim Van Eck. Electromagnetic Radiation from Video Display Units : An Eavesdropping Risk ? *Computers & Security*, 4 (4) :269-286, 1985.
3. Neal Stephenson. Cryptonomicon. 1999.
4. Markus G. Kuhn. Compromising emanations : eavesdropping risks of computer displays. *Technical Report N.577*, University of Cambridge, 2003.
5. Martin Marinov. Remote video eavesdropping using a software-defined radio platform. *Dissertation*, University of Cambridge, 2014.
6. Martin Marinov. TempestSDR. `https://github.com/martinmarinov/TempestSDR`.
7. ANSSI. Instruction Interministérielle n°300 : protection contre les signaux compromettants. 2014. `https://www.ssi.gouv.fr/uploads/IMG/pdf/II300_tempest_anssi.pdf`.
8. Martin Vuagnoux et Sylvain Pasini. Émanations Compromettantes Électromagnétiques des Claviers Filaires et Sans-fil. In *SSTIC*, 2009.