CRM 2010 - Note de synthèse

Télévision interactive (iTV) :

Quelle menace pour la vie privée ?

Auditeur : LEFEBVRE Stéphanie

Directeur de l'Unité d'Enseignement : Professeur BAUMARD Philippe

INTRODUCTION

Ces dix dernières années le téléviseur a connu une évolution sans précédent, passant d'un objet à usage unique bien défini (regarder des programmes analogiques diffusés par les chaines hertziennes) à une plateforme multimédia. En 2017[1], 94% des foyers français possèdent une télévision. Deux tiers des téléviseurs sont potentiellement connectables à internet. 56.3% des foyers reçoivent les programmes par la voie hertzienne ; 25% grâce à une antenne râteau ; 8 téléviseurs connectés sur 10 réceptionnent les chaînes grâce aux décodeurs fournis par les fournisseurs d'accès à internet, via une box (cf annexe 1).

Le marché des téléviseurs a connu une croissance exponentielle[2] ces 5 dernières années. Après une année 2016 records, les fabricants comptent sur les innovations[3] pour réaliser de nouvelles ventes. Celles-ci sont nombreuses tant au niveau du design (développement de « télé incurvées ») qu'au niveau de la qualité de l'image (3D, Ultra HD, 4K[4] (Cf annexe 2)). Même si les moyens de s'informer ne passent plus par la télévision, que les smartphones et tablettes permettent eux aussi de se divertir et font baisser le temps passer devant le téléviseur, cet objet perdure dans les foyers notamment grâce de console de jeux vidéo[5] et aux nouveaux services qu'une connexion internet offre. Au niveau mondial, 59% des téléviseurs achetés sont connectables à internet. Le budget télé mondial est estimé à 100 milliards d'euros[6] et la dépense moyenne pour l'achat d'une télévision est de 440 euros.

L'évolution technologique a transformé un objet quotidien, grand public, en un hardware sophistiqué offrant une multitude de services et dont les marchés français et mondial sont colossaux. Toute nouvelle technologie de cette ampleur représente une aubaine pour les cybercriminels. Pour cette raison, il est indispensable de savoir comment ces téléviseurs fonctionnent (I), d'en identifier les vulnérabilités (II) puis de voir ce que la loi prévoit (III), avant de proposer des recommandations (IV).

---

1 http://www.csa.fr/Etudes-et-publications/Les-observatoires/L-observatoire-de-l-equipement-audiovisuel-des-foyers/L-equipement-audiovisuel-des-foyers-des-1er-et-2eme-trimestres-2017-pour-la-television

2 https://www.usine-digitale.fr/article/5-8-millions-de-televiseurs-vendus-en-france-en-2014-le-marche-repart-legerement-a-la-hausse.N311585 5.8 millions de téléviseurs vendus en France en 2014

3 http://www.francetvinfo.fr/economie/consommation-le-marche-des-televiseurs-en-berne_2379681.html

4 http://newsbytes.ph/2015/04/21/global-4k-display-market-to-reach-52-billion-in-2020/

5 http://www.europe1.fr/technologies/ps4-xbox-one-wii-u-3ds-ou-en-est-le-marche-des-consoles-de-jeux-video-2655191

6 http://www.gfk.com/fr/insights/press-release/les-smart-tv-gagnent-du-terrain/

I - FONCTIONNEMENT DE L'iTV

L'iTV, aussi appelée SmartTV, est nécessairement connectée à internet. Elle ne se constitue plus d'un simple écran, des ports USB, une caméra, un microphone lui ont été ajouté et du contenu additionnel est ajouté aux programmes par les émetteurs.

La caméra peut être utilisée pour réaliser des visioconférences ou pour contrôler le changement de chaîne ou de volume d'un simple geste. Pour que cela soit possible, il est nécessaire que la caméra reconnaisse le ou les individus installés devant l'iTV. Pour se faire, les télévisions sont équipées de systèmes identiques à ceux de Kinect[7] (cf annexe3). Cette reconnaissance permet de se connecter à des comptes, tel que le service SmartHub proposé par Samsung, disponible sur tous les appareils susceptibles d'avoir une connexion internet.

Afin que la SmartTV puisse être utilisée par n'importe quel consommateur, il a fallu harmoniser les canaux d'émission des flux télévisuels et internet. A l'échelle européenne, cela a été réalisé dès 2010, par ETSI[8], au travers d'une norme constructeur[9] qui donna naissance au protocole « Hybrid Broadband Broadcast Television[10] » dont l'acronyme est HbbTV. Ce protocole permet d'ajouter du contenu grâce à une page HTML, dont l'adresse URL sera spécifiée si la télé est connectée à internet ou dont le contenu sera directement ajouté au flux si la télé n'est pas connectée.

L'ETSI fixe également d'autres recommandations :

- Le signal peut être transporté par le Broadcast ou au format HTTP
- Les formats audios et vidéos doivent correspondre à ceux définis par l'OIPF
- Les applications doivent être en langage XHTML, CSS et JavaScript pour les API
- Les images doivent avoir un certain format
- Compatibilité avec d'autres appareils

L'utilisation de certains services ou applications nécessitent la création d'un compte utilisateur, comportant de nombreuses informations personnelles sensibles (nom, prénom, date de naissance, adresse mail, numéro de carte bancaire, mot de passe, etc.) qui sont associés à une adresse IP pouvant être géolocalisée. A cela peut s'ajouter des données encore plus personnelles telle que la reconnaissance faciale, possible grâce à la caméra intégrée (Cf annexe : fonctionnement de la caméra).

II – VULNERABILITES DE L'iTV

Pour prendre connaissance des vulnérabilités d'un tel système, il est nécessaire de le représenter d'un bout à l'autre de la chaîne, de l'acquisition des données, à l'aide de la caméra, jusqu'aux serveurs des entreprises commercialisant le dispositif (Cf Schéma en annexe).

L'iTV est vulnérable à plusieurs niveaux :

- **Niveau du hardware** : les ports USB sont une porte d'entrée très facile à utiliser pour quiconque a accès au téléviseur quelques minutes. Ainsi, l'attaque peut être ciblée et

7

8 Europena Telecommunications Standards Institute http://www.etsi.org/

9 ETSI TS 102 796 V1.1.1 (2010-06) fût la première version, la dernière date de janvier 2017

10 http://www.etsi.org/technologies-clusters/technologies/broadcast/hybrid-broadcast-broadband-television

commise par un proche ou un faux-dépanneur. Dans ce cas de figure, il y a de fortes chances que cette attaque serve surtout à espionner les habitants du foyer ;

- **Niveau du réseau** : attaque de type « man in the middle », les box des FAI présentent elles aussi des failles de sécurité[11] ;
- **Niveau du software** : le système d'exploitation n'est jamais totalement sûr, les applications utilisées présentant du code malicieux (malware), des failles de sécurité ou peuvent être développées dans le seul but de compromettre le système. Ce type d'attaque repose essentiellement sur de l'ingénierie sociale.

Les attaques utilisant la partie software du dispositif peuvent être les suivantes :

- **Fraude au clic** : création de spam qui invite l'utilisateur à cliquer sur des liens qui peuvent être sans danger. L'arnaqueur est juste rémunéré au nombre de clics. Cette méthode est gênante mais peu risquée pour l'utilisateur ;
- **Botnet** : la télévision est utilisée pour réaliser des attaques de type DDoS[12]. Cela est possible car les mots de passe constructeur sont très faibles et uniques pour l'ensemble d'une marque[13] et que l'utilisateur ignore bien souvent qu'un mot de passe existe et qu'il doit être changé dès l'installation du téléviseur. De plus, l'absence de clavier rend difficile le choix d'un mot de passe complexe[14], robuste, qu'il sera nécessaire d'entrer à chaque connexion ;
- **Vol de données personnelles sensibles** : Ex : certaines applications peuvent nécessiter l'enregistrement d'un moyen de paiement telle qu'une carte bancaire. Voler de telles données permet de réaliser des achats frauduleux, de tout type, y compris illégaux. Elles sont aussi revendues sur le darkweb ;
- **Minage de crypto-monnaies** : la télé peut être utilisée pour miner[15] des crypto-monnaies, tel que des bitcoins. La puissance de calcul est certes très faible par rapport à un ordinateur mais à grande échelle cela devient intéressant car rentable ;
- **Rançongiciel** : le hacker crypte et bloque l'accès de la télévision et promet de rentre l'accès contre le paiement d'une rançon s'élevant à quelques centaines d'euros. La tentation de payer la somme demandée est forte car elle semble faible par rapport au coût d'achat d'un nouvel appareil. Le cryptage d'une télé n'est pas très rentable, mais là encore le nombre de victimes potentielles est tellement important que ce système devient vite très lucratif.
- **Accéder à d'autres appareils connectés** : l'iTV devient une porte d'entrée[16] vers le réseau internet privé, permettant d'infecter tout objet qui y est connecté (ordinateur, smartphone, gadgets de toute sorte). Il existe des applications permettant de transformer le smartphone en télécommande ;

---

11 http://www.rtl.fr/actu/futur/une-faille-de-securite-permet-de-pirater-des-box-orange-et-sfr-7789687963

12 Attaque DDoS, aussi nommé « attaque par déni de service » vise à saturer les serveurs d'un site, en lui envoyant de très nombreuses requêtes dans un laps de temps très court. La saturation rend le site indisponible aux visiteurs légitimes. https://www.infohightech.com/etude-symantec-des-attaques-ddos-toujours-plus-rapides-et-intenses-les-objets-connectes-en-ligne-de-mire/

13 Le mot de passe par défaut des télévisions de la marque Samsung vendues en France est 1111

14 https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf

15 Les cryptomonnaies sont des devises dites décentralisées, il n'y a donc pas de serveur pour contrôler le tout. Ainsi, chaque système informatique travaillant sur le monnaie dispose d'une copie du registre général référençant toutes les opérations (blockchain). Le minage revient à ajouter une brique d'information à la blockchain

16 https://www.symantec.com/connect/blogs/dawn-ransomwear-how-ransomware-could-move-wearable-devices

- **Espionnage audio-visuel** : utilisation des micro et caméra intégrés à la télévision pour espionner le foyer. Par ailleurs, les informations recueillies peuvent être aussi réutilisées pour organiser une attaque plus ciblée ou plus importante. « *D'autres part, les TV ou boitiers qui embarquent une webcam (comme la Xbox One et sa Kinect) et accueillir des applications sont aussi une aubaine pour les pirates qui pourraient introduire un dispositif de surveillance à votre insu.* »[17].

L'iTV peut également posséder une porte dérobée communément nommé « backdoor ». Ces backdoors intégrées au code source originel du téléviseur, par le fabricant, permet de réaliser des actions à l'insu du téléspectateur[18]. Ces actions ne sont pas nécessairement malveillantes. Ainsi lors d'un audit effectué en 2015 un code nommé « wifatch [19]» a été trouvé son objectif était de stopper les logiciels malveillants déjà installés sur la télévision.

Les attaques à partir du hardware nécessitent un accès physique aux matériels. Un microprocesseur monté sur un objet identique en apparence à une clé USB permet l'exécution d'un code malveillant qui va compromettre le téléviseur. Mais un accès physique au réseau est également possible au niveau du raccordement de l'opérateur internet au bâtiment du téléspectateur. Lorsque l'opérateur Orange a été informé de cette menace il a répondu ceci : « *Nous soulignons qu'il y a aucun danger pour nos clients et que l'opération décrite ne peut pas se faire à distance, il faut être physiquement chez l'abonné ce qui réduit considérablement sa portée*. »[20], ce qui démontre le peu d'implication des fournisseurs dans la sécurité de leurs clients.

Les attaques que nous avons citées précédemment ne sont pas spécifiques aux téléviseurs, elles peuvent être perpétrées sur des ordinateurs, des smartphones, ou encore des tablettes. Comme nous l'avons vu plus haut, les téléviseurs ont des spécificités tel que le protocole HbbTV offre d'autres opportunités d'attaques que nous classerons dans la catégorie « attaque du réseau internet ». Cette harmonisation créée une homogénéité des systèmes qui, en soi, crée une vulnérabilité réseau : une même attaque peut être utilisée sur tous les téléviseurs.

L'une des caractéristiques de cette harmonisation est au, par défaut, la télévision se connecte systématiquement au signal le plus fort. Le signal émis par les chaînes est très fort mais très diffus et éloigné de chaque téléviseur. Il devient facile de le surpasser en puissance simplement en émettant un signal plus proche de l'iTV. Ainsi, des attaques utilisant les signaux DVB-T peuvent être réalisées pour un coût de 100 euros depuis un immeuble voisin de la personne ciblée à l'aide d'un drone. Ce type d'attaque permet de contrôler le téléviseur, sans que l'utilisateur légitime s'en aperçoive[21].

Les attaques du réseau DVB peuvent avoir des conséquences sur l'utilisateur mais aussi, à plus grand échelle, sur un émetteur. Par exemple si le flux de la chaine TF1 est totalement corrompu un soir de diffusion de match de football de coupe du monde, l'impact financier et sur l'image du diffuseur peut

17 http://forums.cnetfrance.fr/topic/1205904-smart-tv--comment-securiser-sa-tele-connectee/
18 Cette porte dérobée a possiblement été utilisé
19 https://www.symantec.com/connect/blogs/there-internet-things-vigilante-out-there Le code source de ce programme est en accès libre à cette adresse : https://gitlab.com/rav7teif/linux.wifatch
20 http://www.zdnet.fr/blogs/infra-net/d-inquietantes-failles-de-securite-dans-les-acces-fibre-optique-ftth-en-france-39844258.htm
21 https://www.developpez.com/actu/127805/Un-chercheur-en-securite-developpe-une-attaque-permettant-de-pirater-a-distance-une-television-connectee-et-espionner-son-proprietaire/

être catastrophique. Les différentes attaques sont regroupées et présentées dans un tableau en Annexe.

III – CADRE LEGAL / JURIDIQUE

En droit français, la vie privée est protégée par l'article 9 du code civil et l'article 226-1 du code pénal. Les sanctions sont à la fois financières (amende pouvant aller jusqu'à 45 000 euros) et privatives de liberté (un an d'emprisonnement et confiscation du matériel ayant servi à commettre l'infraction). En matière informatique, des sanctions plus spécifiques sont prévues par la loi Godfrain[22] du 5 janvier 1988. Depuis son entrée en vigueur cette loi a régulièrement été enrichie pour correspondre à l'évolution[23] des menaces cyber.

Dans les faits, le cyber-délinquant n'est pas la seule préoccupation vis-à-vis du respect de la vie privée. Samsung dispose, dans ses notices d'utilisations, que « l'utilisation de ses produits équivaut à l'acceptation des condition générales d'utilisations » et que « seul l'utilisateur est responsable des utilisations malveillantes, pour la vie privée, de ses produits ». Comme l'a démontré l'enquête récente en Belgique *« la plupart des utilisateurs accordent leur consentement sans même s'en rendre compte »* [24]. Franck Cormerais[25] va plus loin en disant « *La servitude volontaire se manifeste par un clic, celui de l'obtention d'un consentement, lorsqu'on utilise des services sur internet. […] Aujourd'hui, probablement, il y a une quasi extorsion du consentement ; […] on est plutôt dans l'ordre de l'insu, de la dimension non réfléchie que je donne à mes actes*. »[26] . Or ces données sont destinées à produire de la publicité ciblée et à construire un profilage des téléspectateurs. Ce type de données étant tellement important, collecté par tous les acteurs commerciaux qui se réservent le droit de se les revendre entre eux[27], que le réel anonymat est quasiment impossible. Le recoupement de seulement quelques informations à caractère personnel[28] suffit à identifier un individu et donc de ne plus respecter sa vie privée. Le risque est d'autant plus important qu'il ne s'agit plus de données qui peuvent être changées, tel qu'un mot de passe ou un compte utilisateur, mais relève de l'identité de l'individu au travers de son patronyme et de sa biométrie.

En France, la CNIL encadre, grâce à la loi n°78-17[29] dite « loi informatique et liberté, la gestion des données personnelles. Ainsi, les données biométriques doivent obligatoirement être stockées localement[30]. Samsung assure que les données biométriques sont placées dans un espace crypté et séparé de ses appareils[31]. Quand aux autres types de données, bien souvent elles sont stockées sur des serveurs hors de l'Union européenne ne sont plus protégées légalement. Elles pourraient alors devenir la cible privilégiée et en tout impunité de cyberdélinquants.

---

22 https://fr.wikipedia.org/wiki/Loi_Godfrain

23 https://www.observatoire-fic.com/la-loi-godfrain-au-plus-pres-de-lactualite-cybercriminelle-par-le-general-darmee-2s-watin-augouard/

24 https://www.rtbf.be/info/societe/onpdp/detail_quel-controle-le-consommateur-a-t-il-sur-sa-smart-tv?id=9748078

25 **Franck Cormerais** est professeur à l'université Bordeaux-Montaigne. Il est l'auteur de plusieurs ouvrages sur la communication et a dirigé plusieurs recherches collectives relatives au numérique.

26 https://www.franceculture.fr/emissions/entendez-vous-leco/entendez-vous-leco-mercredi-29-novembre-2017

27 https://privacy.microsoft.com/fr-fr/privacystatement

28 https://www.cnil.fr/fr/definition/donnee-personnelle

29 https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460

30 https://www.cnil.fr/fr/smartphone-authentification-avec-vos-donnees-biometriques

31 E-manual Samsung

En mai 2018 entrera en vigueur le General Data Protection Regulation[32] (GDPR), règlement européen sur les données personnelles. Cette nouvelle législation oblige l'utilisateur à donner explicitement son consentement pour l'exploitation de ses données (avec une autorisation parentale obligatoire pour les mineurs): il ne peut plus être tacite ou se déduire de son comportement. Si elles sont piratées, l'entreprise qui les détient doit en informer l'utilisateur dans les 72 heures pour qu'il se protège. Peu importe que cette entreprise soit établie dans ou hors Union européenne car dès qu'elle s'adresse à des citoyens européens elle doit se conformer au GDPR. Un organisme de contrôle et des sanctions sous forme d'amende sur le chiffre d'affaires sont prévus contre les contrevenants[33].

IV - RECOMMANDATIONS

Recommandations à destination des constructeurs :

- Communiquer sur les failles et les risques encourus par l'utilisateur ;
- Surcouche de chiffrement permettant le cryptage de données de bout en bout ;
- Installer des moyens de protections relevant du hardware (ex : cache physique sur la caméra ne pouvant pas être activé informatiquement) ;
- Rendre plus difficile le changement du mot de passe du téléviseur en cas de perte (actuellement il peut être réinitialiser à l'aide de la télécommande) ;
- Meilleure sécurisation physique des installations constructeurs ;
- Proposer un clavier

Recommandations à destination des utilisateurs :

- Changer le mot de passe constructeur dès l'installation du téléviseur ;
- Paramétrer convenablement le téléviseur (désactivation de la caméra, activer le contrôle parental, etc.) ;
- Utiliser des mots de passe unique et robuste : chaque compte, chaque application doit posséder des identifiants et mots de passe unique et complexe ;
- Mettre le matériel et les applications à jour immédiatement après la mise en ligne de patch correctif ;
- Sécuriser le réseau auquel est connecté le téléviseur ;
- Eviter de connecter d'autres appareils (ex : smartphone utilisé comme télécommande) à l'iTV ;

CONCLUSION

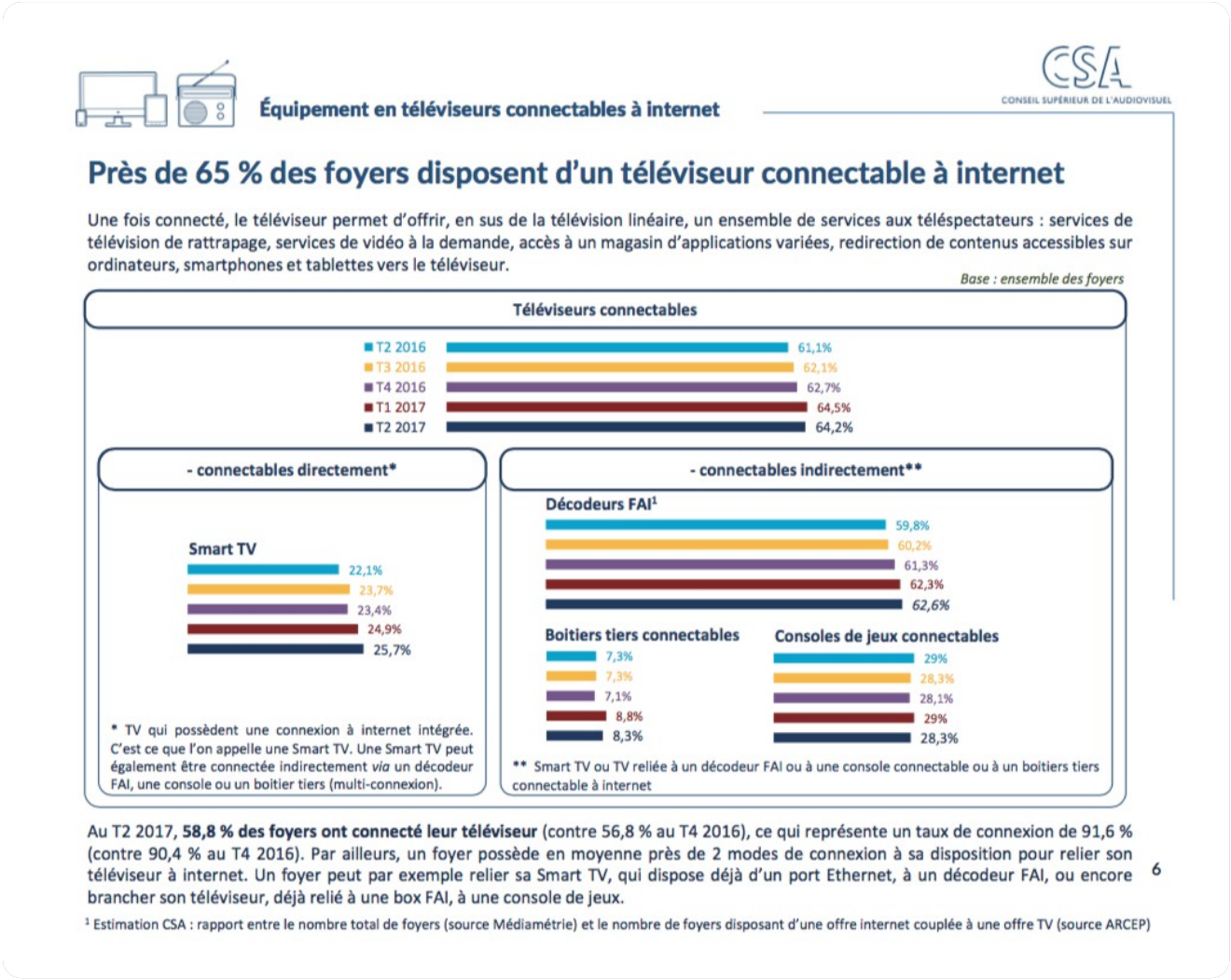
L'iTV a conservé la même fonctionnalité que les téléviseurs cathodiques, à savoir diffuser des programmes à laquelle s'est ajouté une multitude de possibilités. Ces nouvelles fonctions créent des surfaces d'attaque, potentiellement dangereuses pour la vie privée du téléspectateur. Le grand public ignore totalement ce qu'il accepte en installant ce type de matériel à son domicile. Peu de personnes se rendent compte que l'objet, placé au cœur du foyer, accessible à tous les membres de la famille, quel que soit l'âge, et l'heure de la journée ou de la nuit est capable de les espionner, d'enregistrer et transmettre leurs données à caractères personnels et ainsi que des vidéos de leur quotidien obtenues grâce à la caméra et le micro intégrés.

32 http://www.cil.cnrs.fr/CIL/spip.php?article2634
33 https://www.cnil.fr/fr/vigilance-mise-en-conformite-rgpd

Le risque pour la vie privée provient de cyber-attaquants mais aussi des constructeurs et FAI qui utilisent les données confiées par l'utilisateur. La loi et la réglementation suivent les évolutions mais ne les anticipent pas réellement.

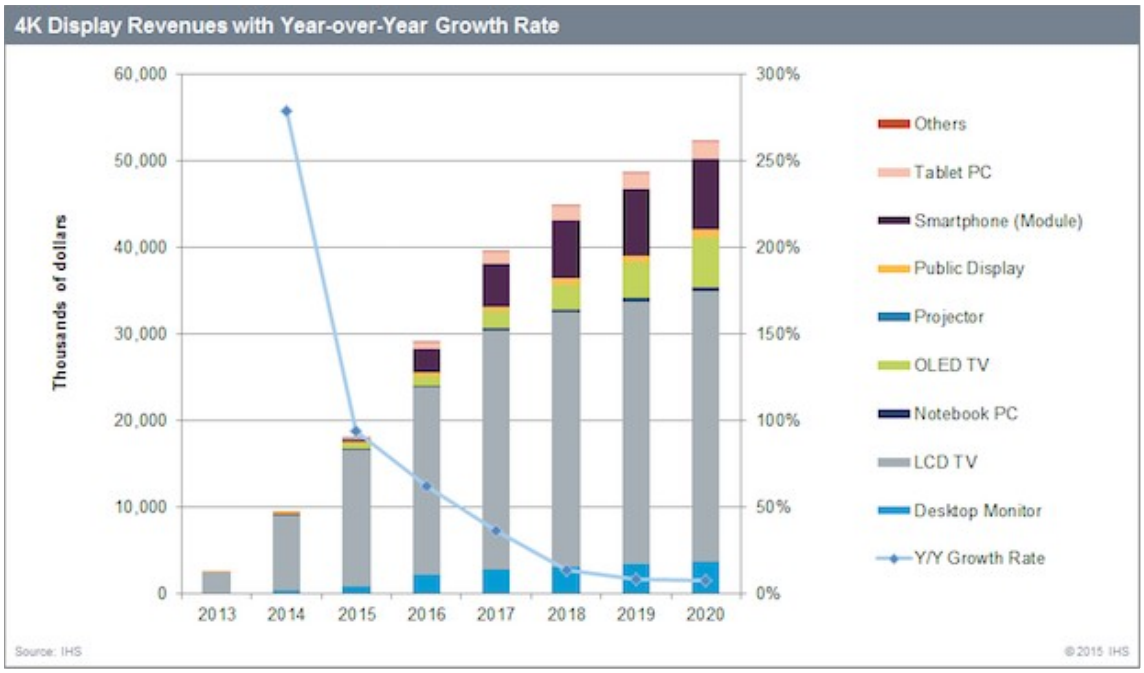
Comme il s'avère très difficile de faire changer les habitudes du téléspectateur-consommateur, il faut que le changement vienne des constructeurs et fournisseurs d'accès à internet. Les fabricants doivent s'assurer que leur modèle soit « secure by design[34] », c'est-à-dire que les architectures informatiques soient pensées à partir d'une méthode formelle.

ANNEXES



Annexe 2 :

34 https://en.wikipedia.org/wiki/Secure_by_design



Annexe 3 : Fonctionnement de la camera integree aux televiseurs

Caméra type deep

Annexe 4 :

Figure 1 depicts the system overview with a hybrid terminal with DVB-S as the example of the broadcast connection.

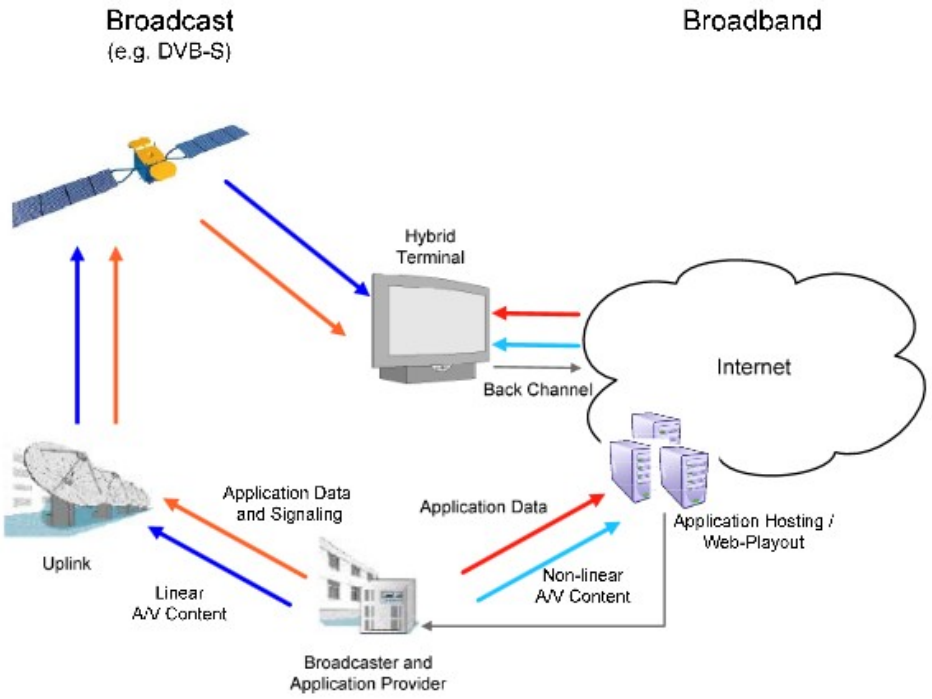


Figure 1: System Overview

Annexe 5 :

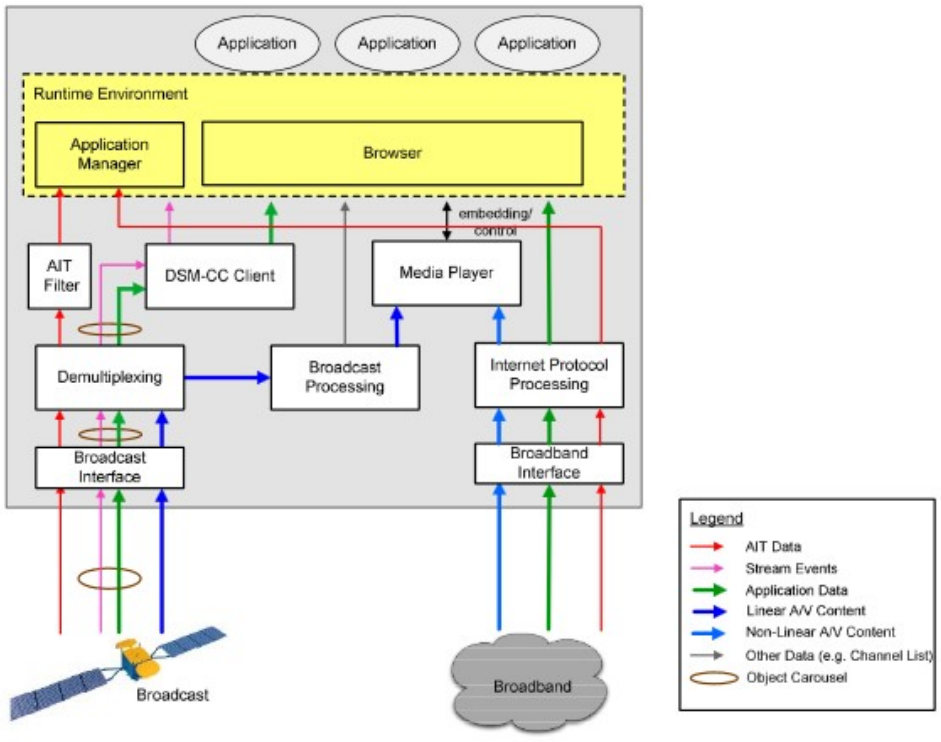


Figure 2: Functional components of a hybrid terminal

Annexe 6 : Tableau récapitulatif des menaces et niveau de dangerosité pour l'atteinte à la vie privée

Point de vulnérabilité	Attaque	Type d'attaque / risque

Port USB	Physique	**Vol de données / Espionnage**
WIFI	A distance	
Applications	A distance	**Vol de données** / **attaque de type rançongiciel**
Canal de diffusion DVB	A distance	**Modification du contenu diffusé par les chaines** / **activation de logiciel malveillant**
Réseau internet	A distance	
Raccordement au réseau	Physique	**Vol de données / Espionnage**
Objets connectés (Console, Disque dur externe, Smartphone,etc)	A distance	**Vol de données / Corruption de l'ensemble du réseau interne et des appareils connectés**
Backdoor	A distance	**Espionnage via la caméra et le micro / vol de données**
Constructeur / Concepteur d'application / FAI	A distance	**Collecte de données / non-respect de la vie privée**