

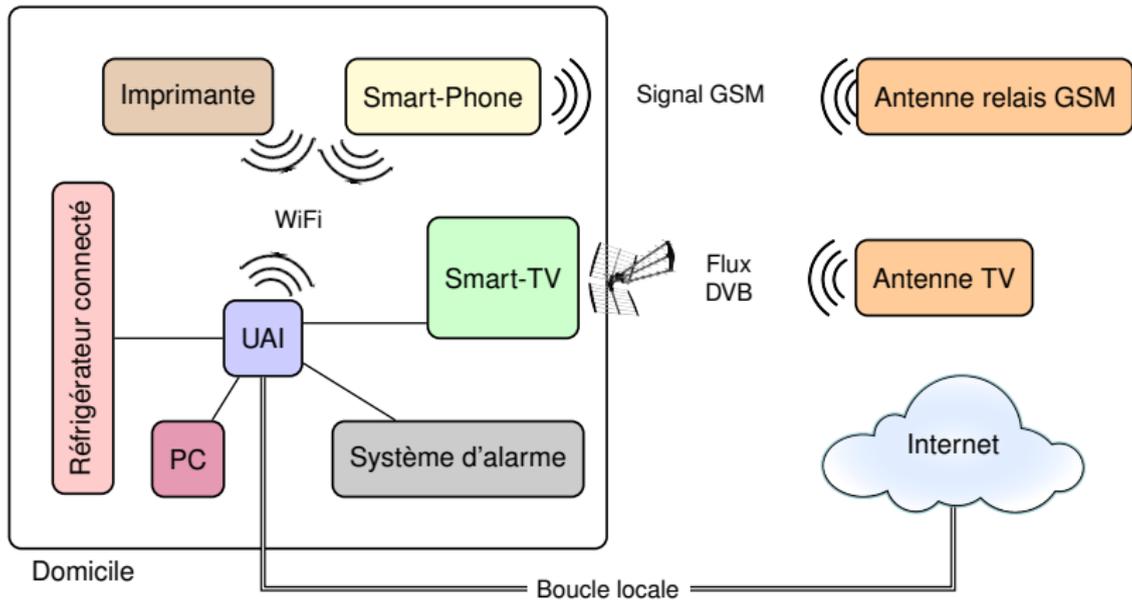


Protocole HbbTV et sécurité : quelques expérimentations

Yann Bachy, Vincent Nicomette, Eric Alata, Mohamed Kaâniche,
Jean-Christophe Courrège et Pierre Lukjanenko

SSTIC 2015

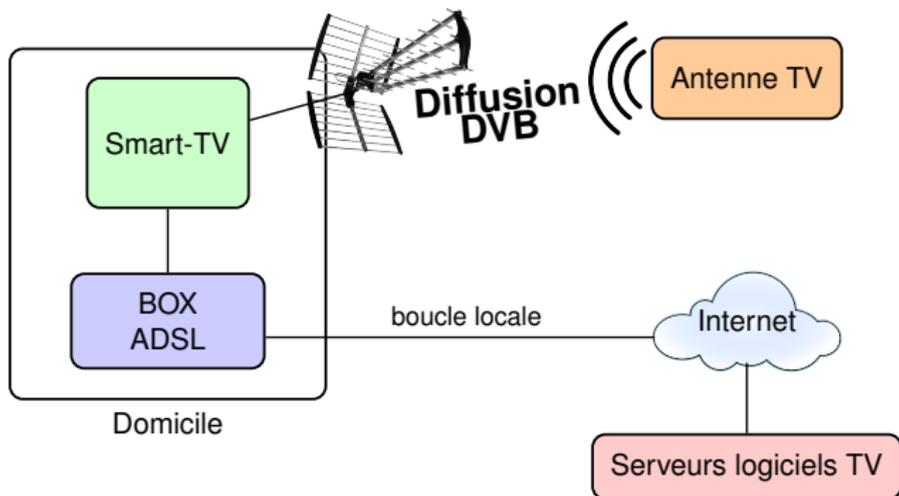


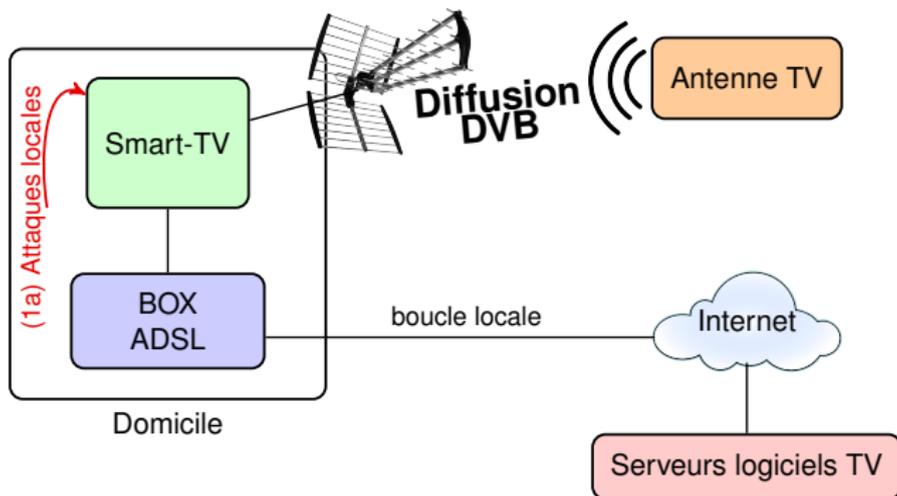


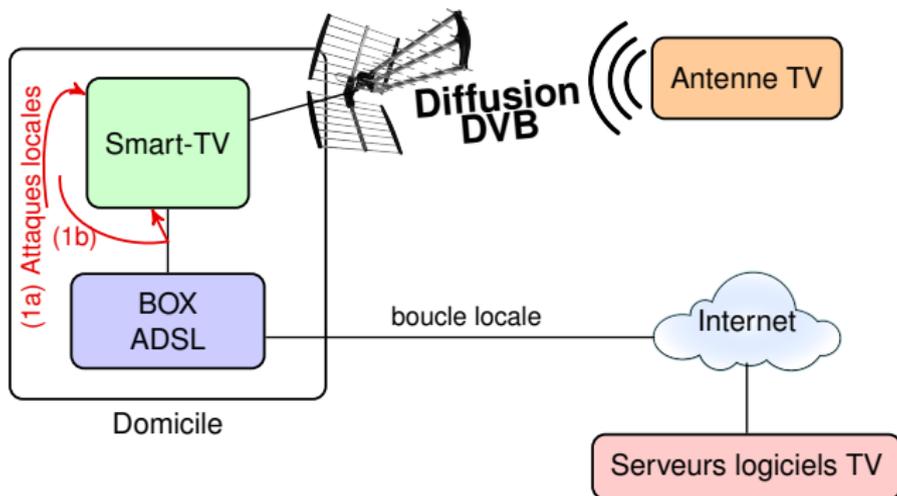
Une Smart-TV présente en plus des fonctionnalités classiques d'un téléviseur les possibilités suivantes :

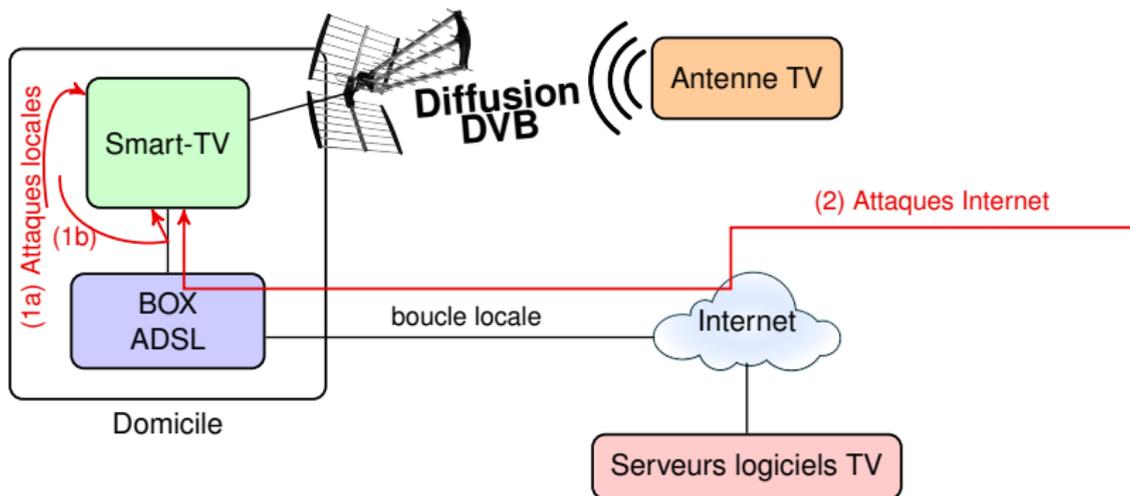
- Une connexion à Internet
- Un ensemble d'applications interactives
 - Navigateur Internet
 - TV à la demande
 - Vidéo à la demande
- Enregistrement numérique
- Lecteur multimédia (réseau)

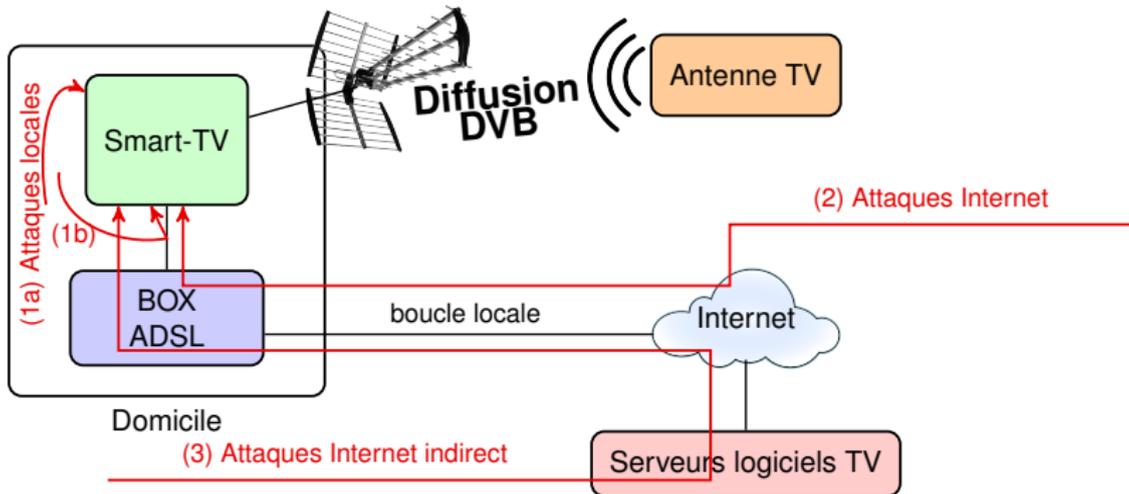
Qu'en est-il de la sécurité ?

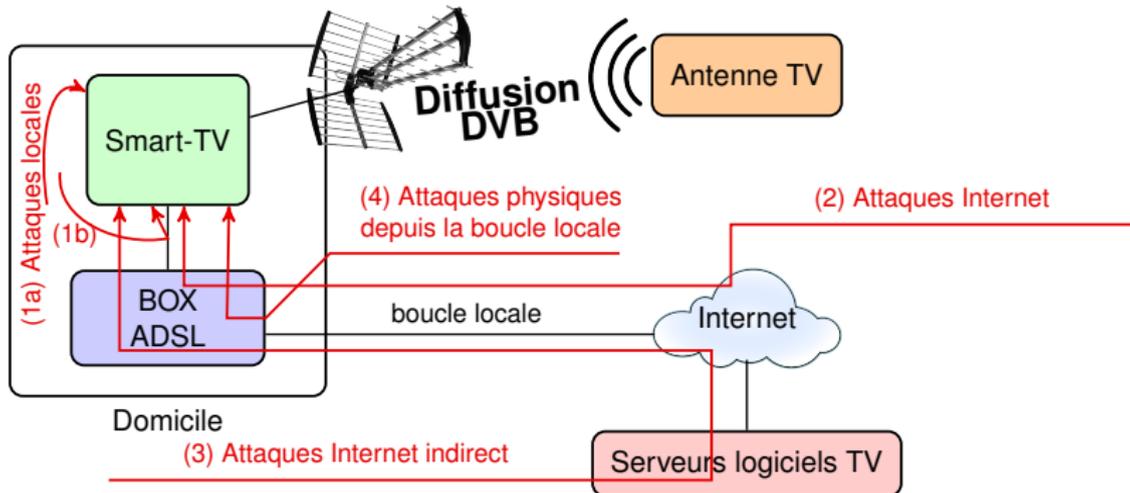


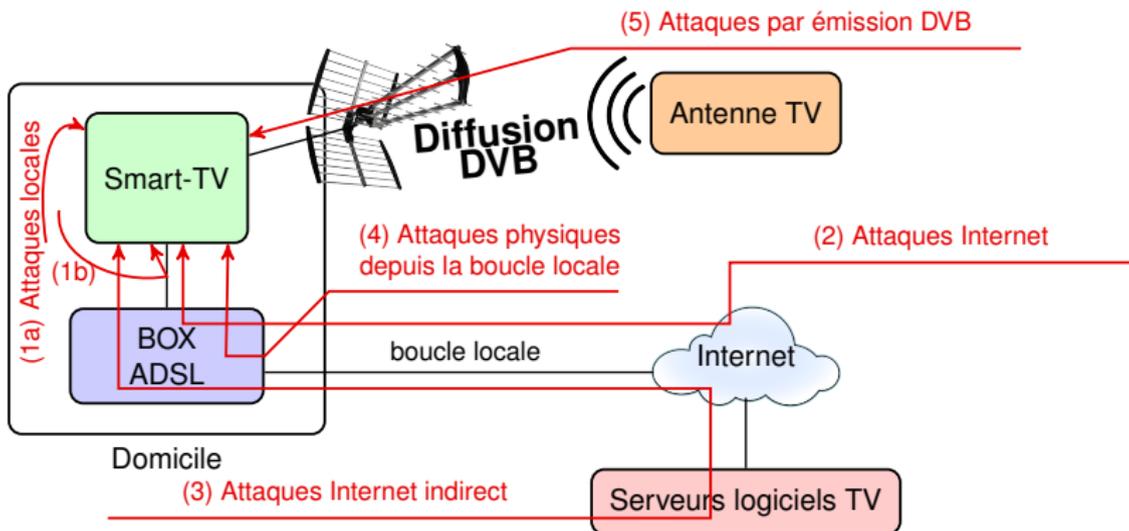


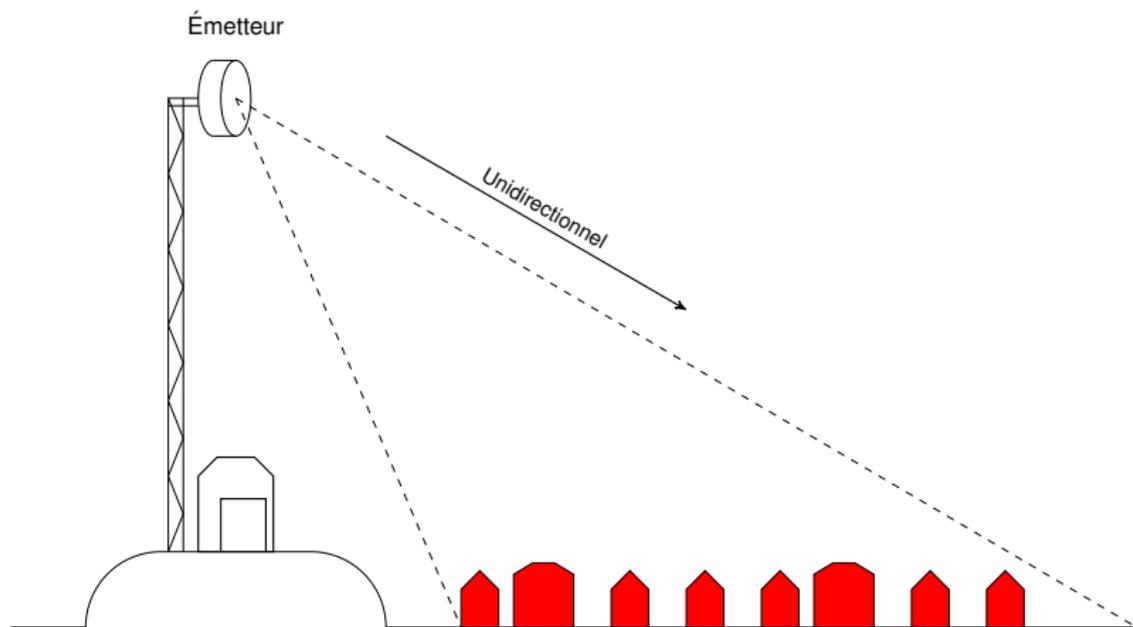








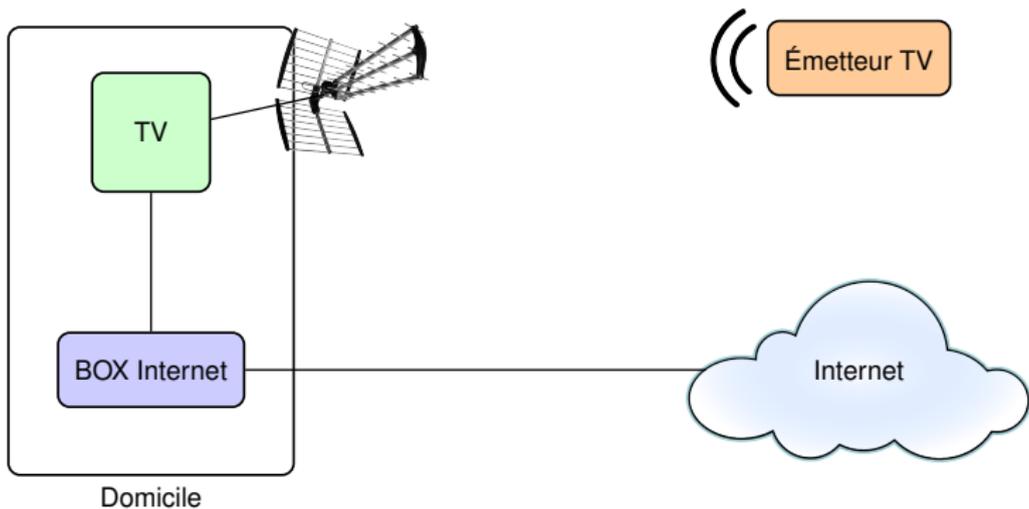


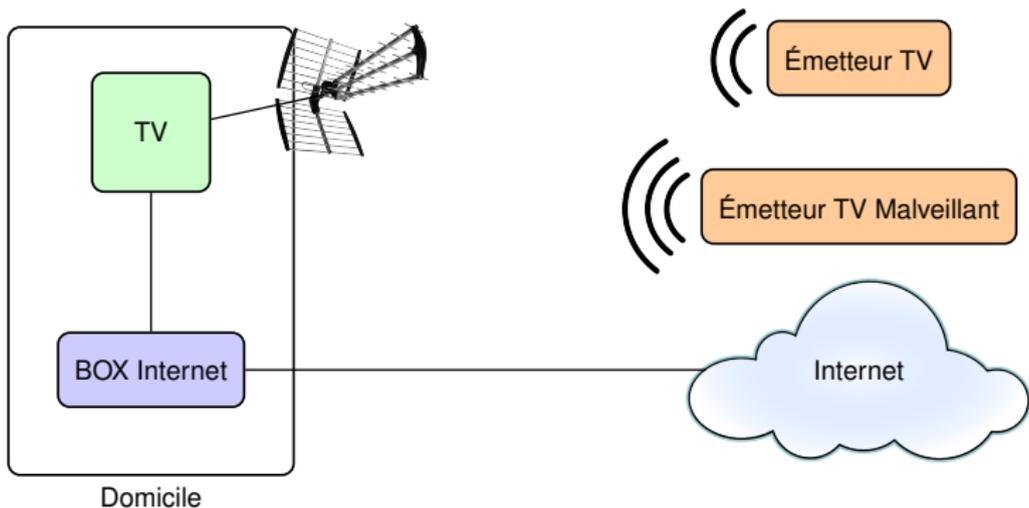


Démonstration 1 :

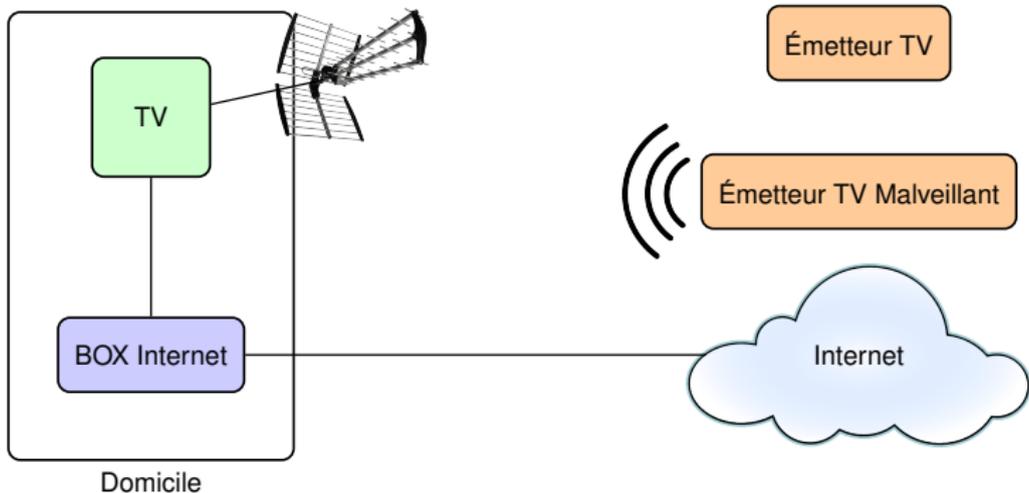
Authentification du signal reçu par un téléviseur ?

(Cette démonstration s'applique à tous les téléviseurs, connectés ou non)





La puissance du signal de l'émetteur malveillant, telle que perçue par le téléviseur, est plus élevée que la puissance du signal émis par l'émetteur légitime.



Le signal de l'émetteur légitime est donc ignoré par le téléviseur.



Démonstration 2 :

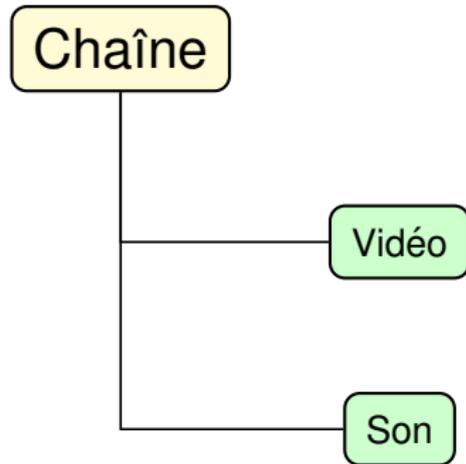
Authentification des données associées à une chaîne ?

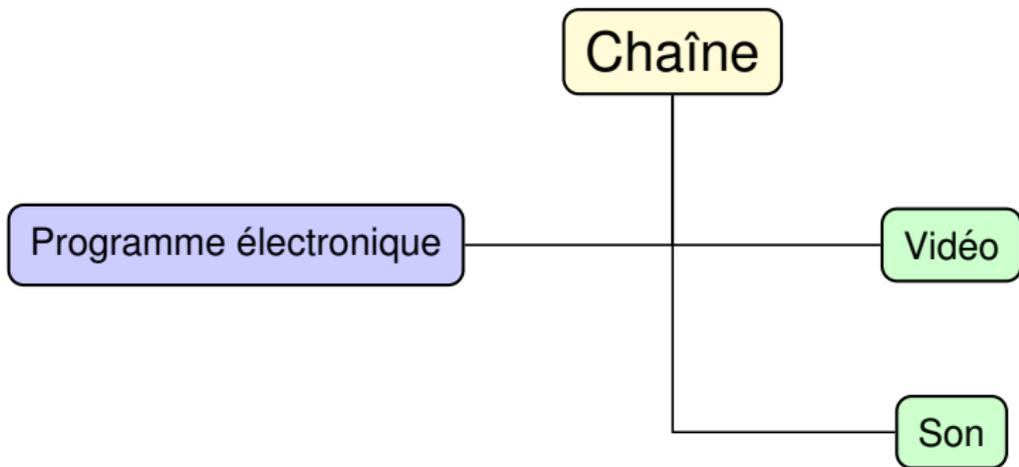
(Cette démonstration s'applique uniquement aux téléviseurs connectés.)

Que contient un flux DVB ?

Chaîne

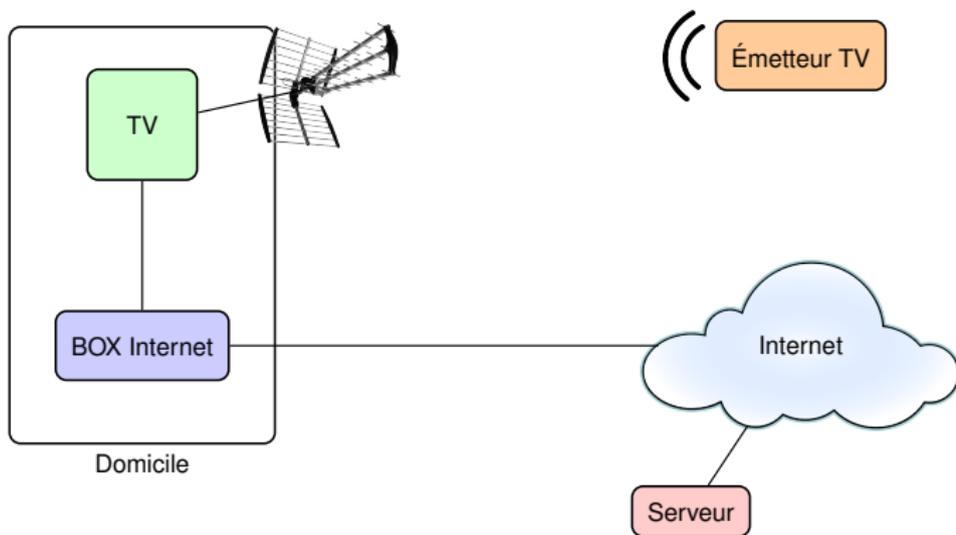
Que contient un flux DVB ?

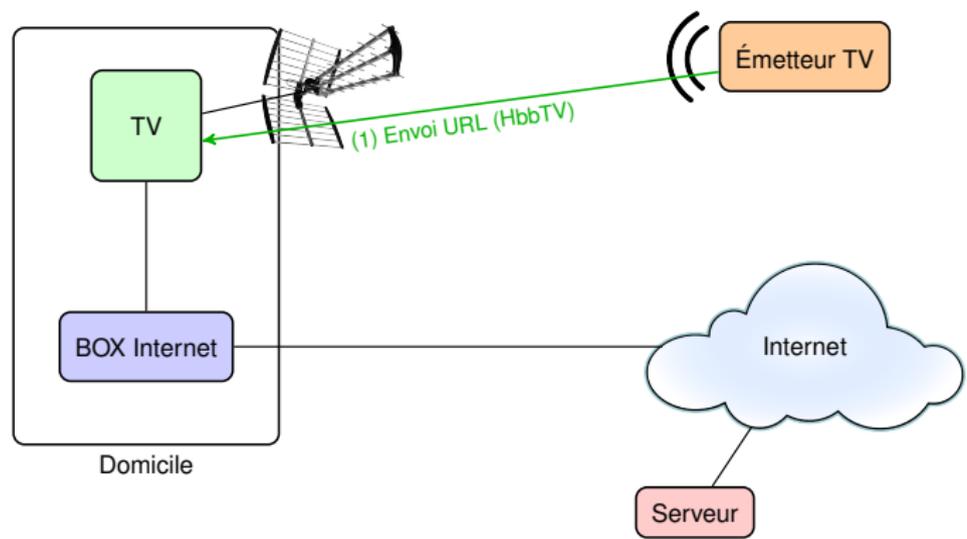


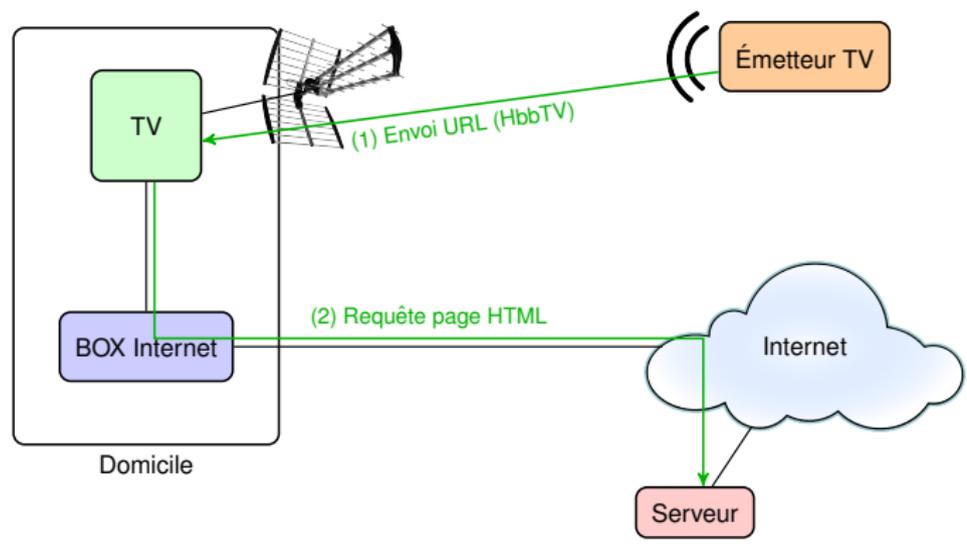


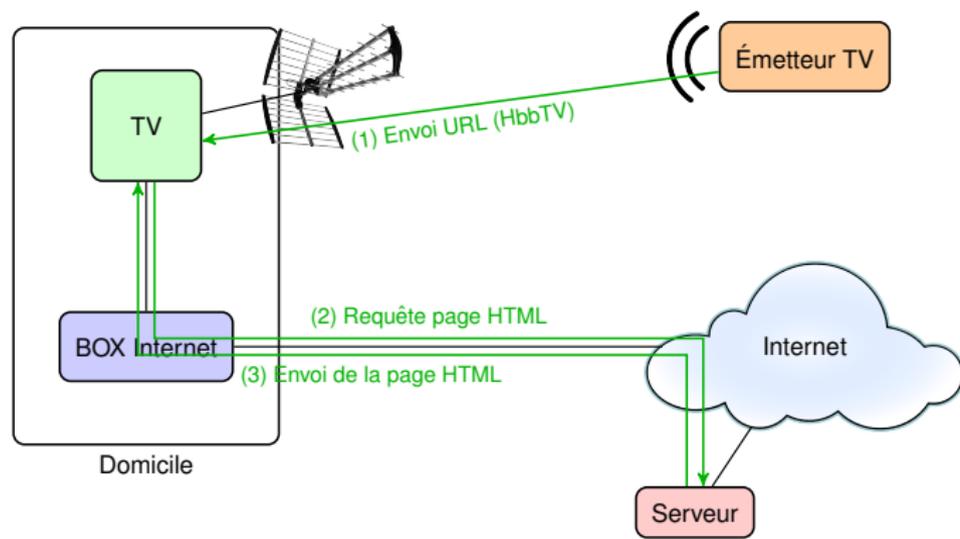
- Informations concernant la chaîne (bouquet, nom, réseau, etc...)
- Informations concernant des "évènements"
- Informations concernant l'heure
- URL de l'**application** associée

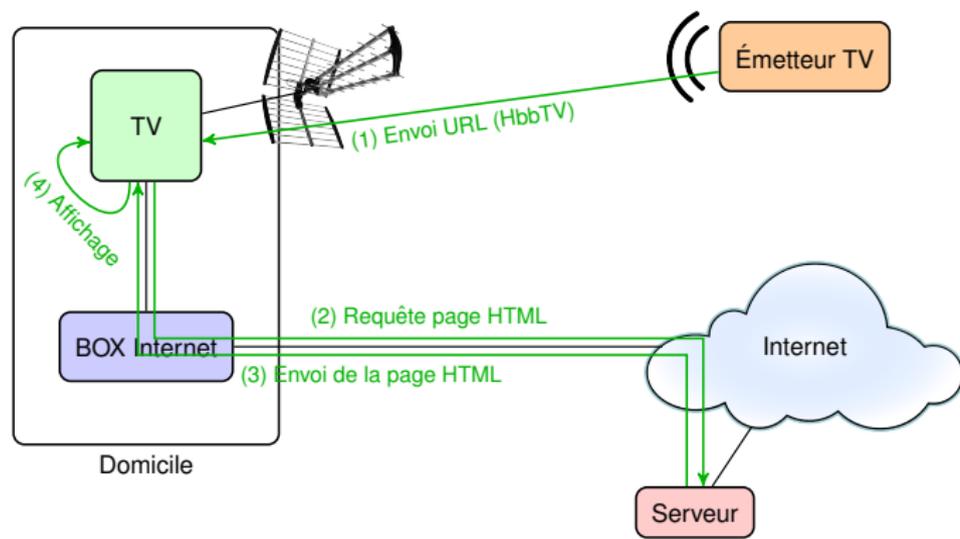
Comment fonctionnent ces **applications ?**

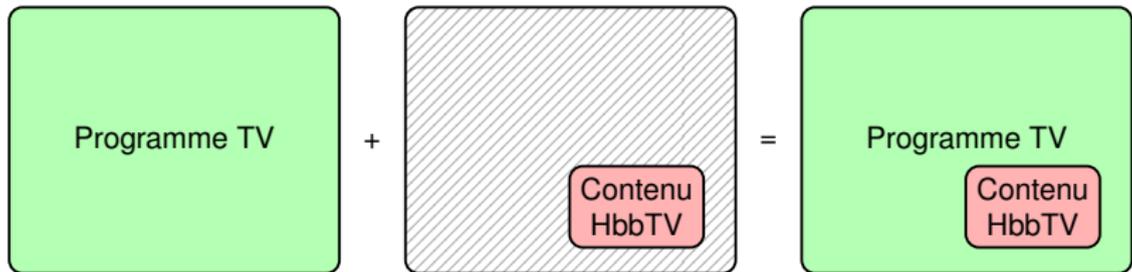






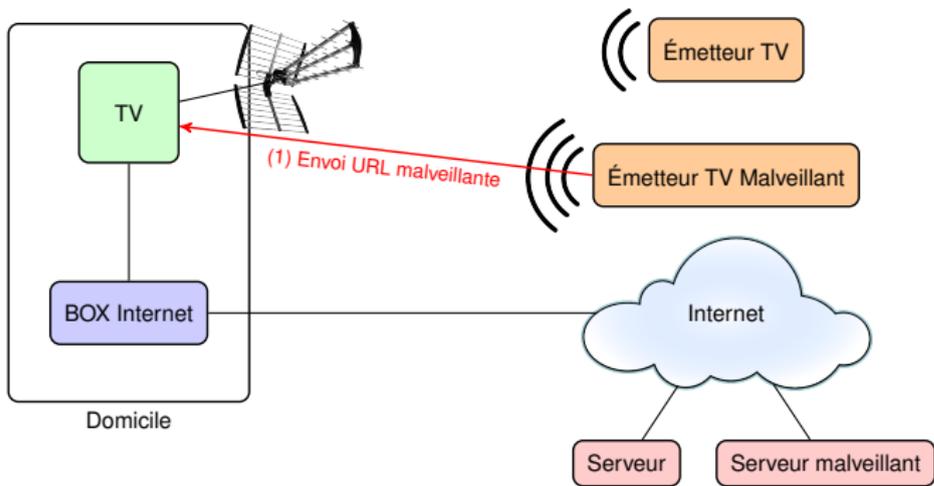


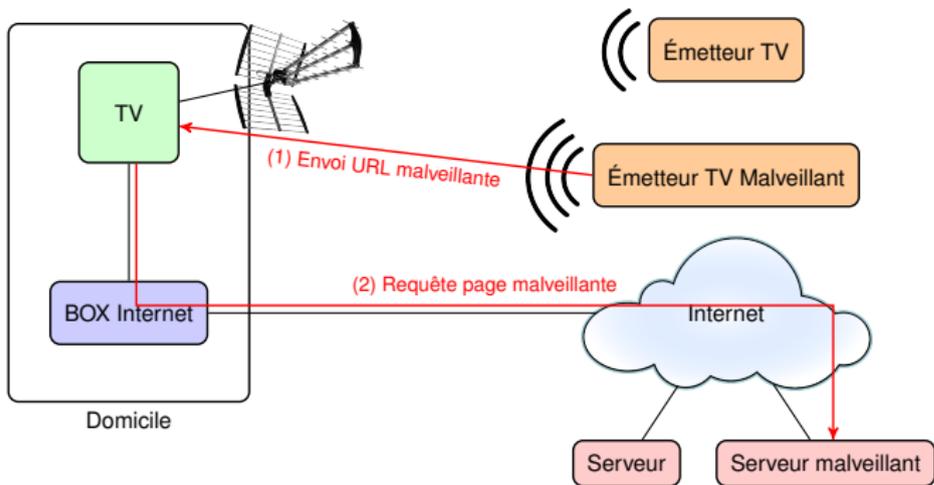


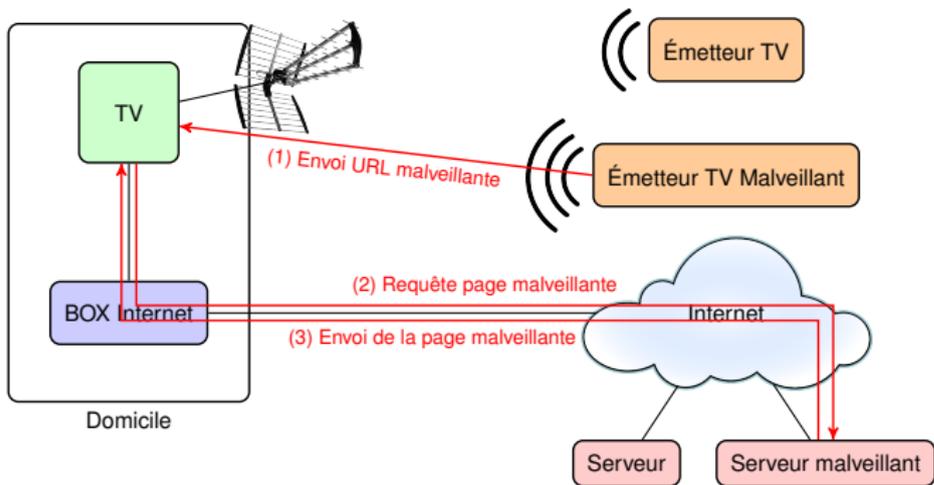


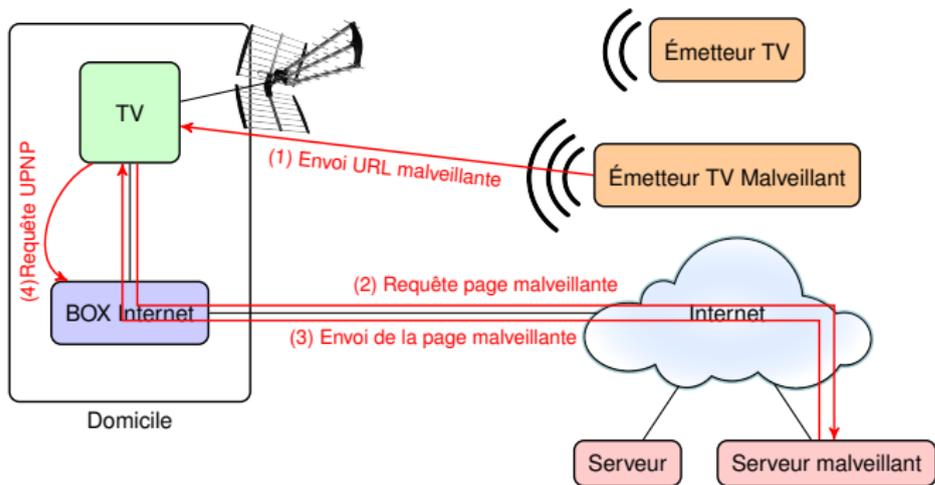
Contenu HbbTV :

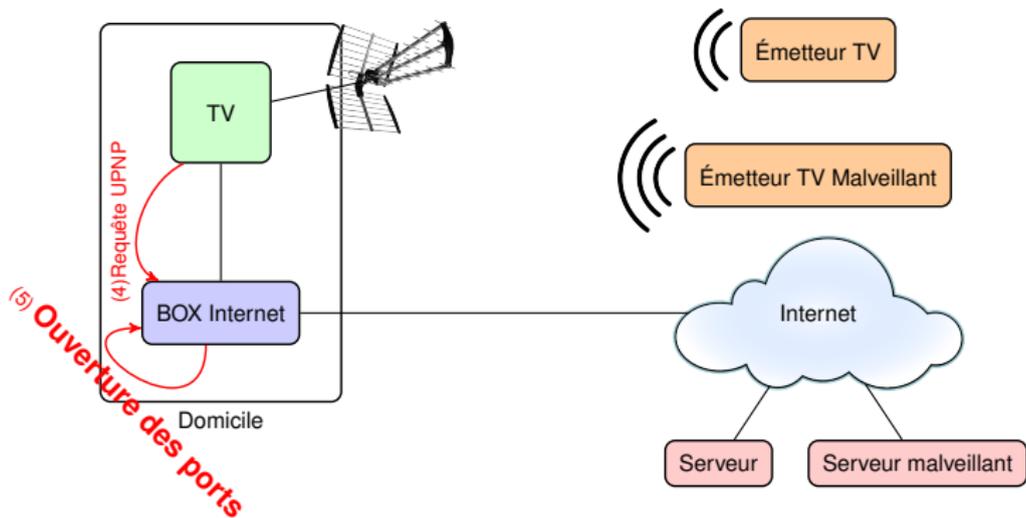
- HTML
- JavaScript
- ...

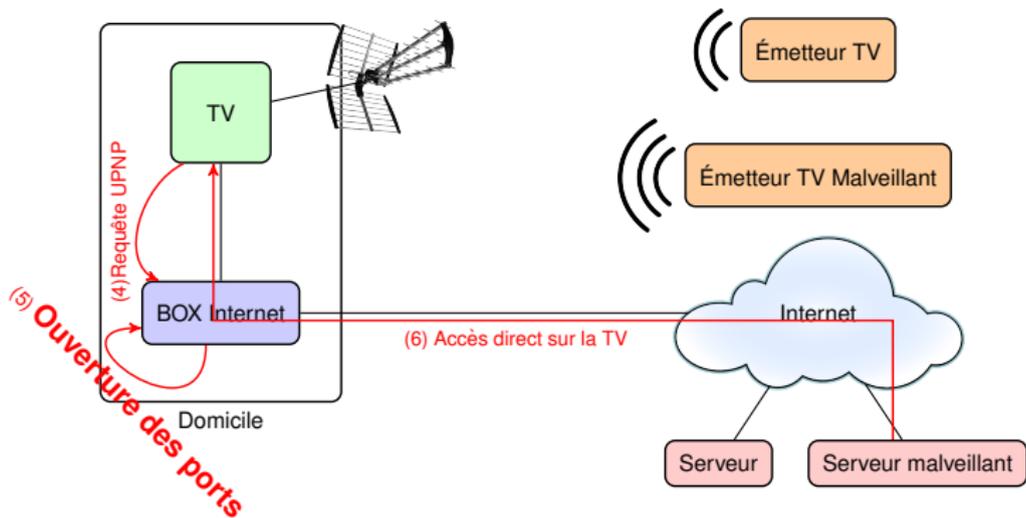


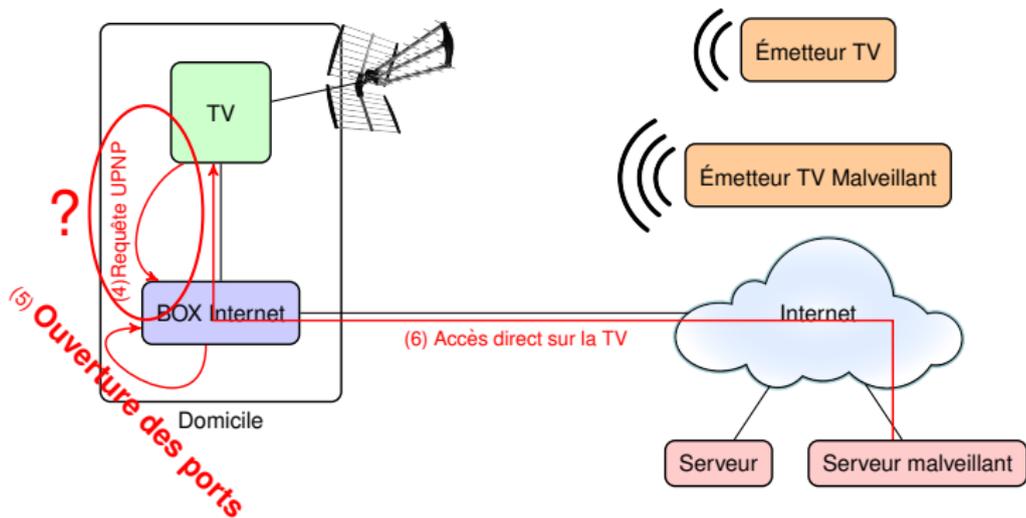












Fonctionnement de la politique de la même origine :



Fonctionnement de la politique de la même origine :



Résultats d'une étude comparative sur 4 téléviseurs :

TV	A	B	C	D
HbbTV	POST	Ignore	OPTIONS	OPTIONS

Fonctionnement de la politique de la même origine :

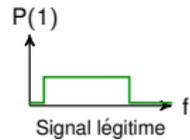
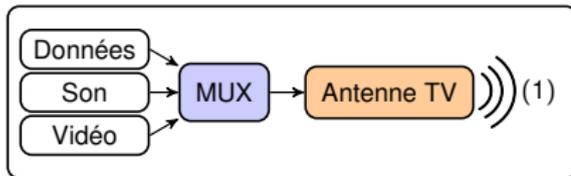


Résultats d'une étude comparative sur 4 téléviseurs :

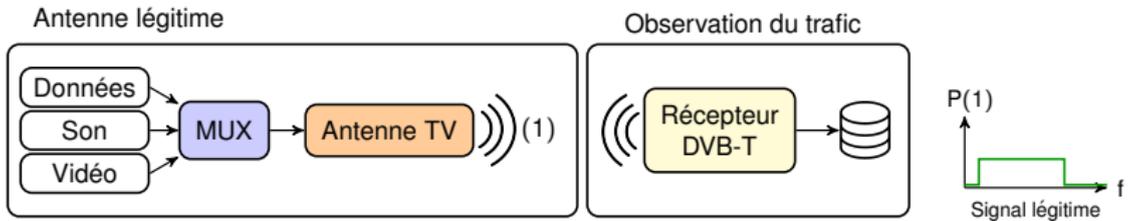
TV	A	B	C	D
HbbTV	POST	Ignore	OPTIONS	OPTIONS
Navigateur	Ignore	OPTIONS	OPTIONS	POST



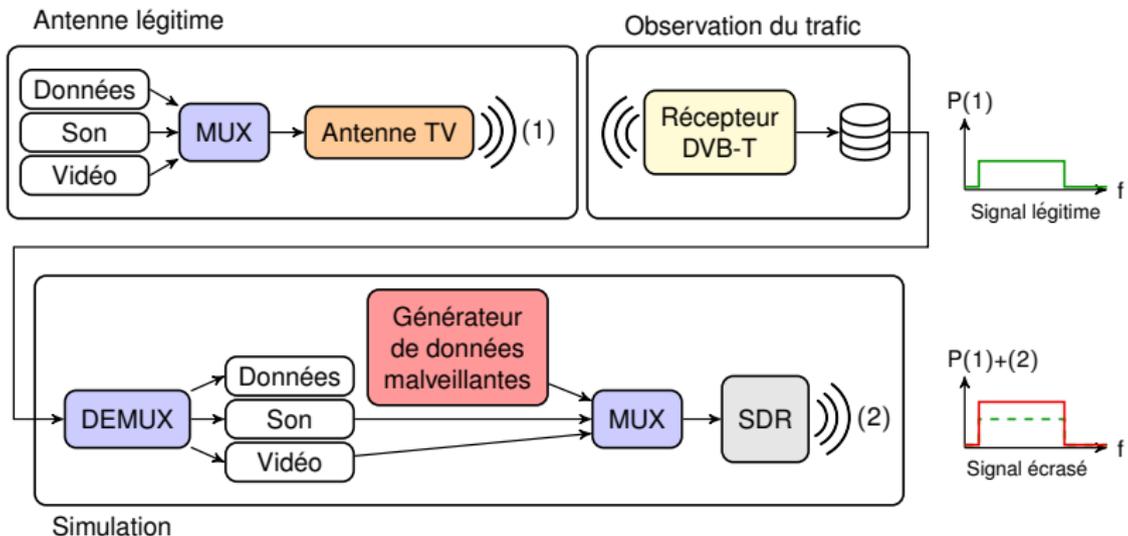
Antenne légitime



(1) = Signal légitime



(1) = Signal légitime



(1) = Signal légitime

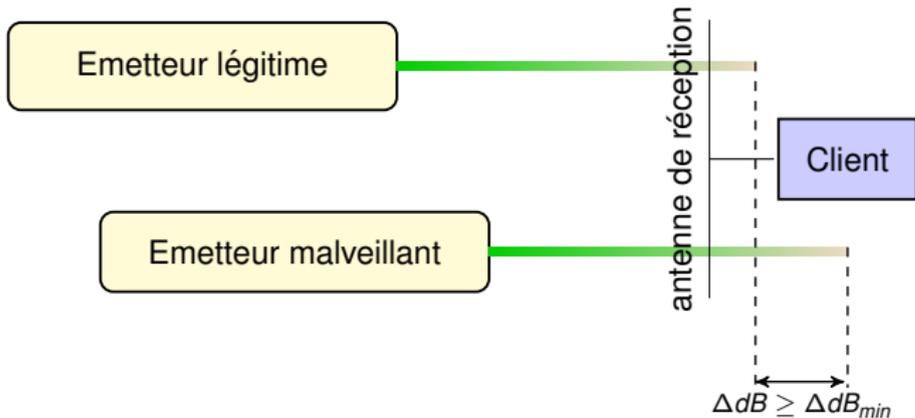
(2) = Signal malveillant

Peu de mécanismes de sécurité prévus dans la norme DVB

Cependant on pourrait :

- Obliger l'utilisation de HTTPS systématiquement lors de l'envoi de contenu HbbTV.
- Insérer régulièrement une somme de contrôle signée de tout le multiplex DVB.
- Surveiller la qualité du signal perçu par le téléviseur (cf. slide suivant).

Surveiller la puissance du signal perçue :



ΔdB_{min} = seuil défini par la norme du protocole.

Conclusion

- La sécurité pas toujours au rendez-vous dans les équipements grand-public connectés à Internet.
- Pas de réels mécanismes de sécurité existants.

Perspectives

- Étendre ce type de travaux à d'autres équipements grand public.
- Couvrir d'autres surfaces d'attaque que les liens de communication (firmware, matériel, ...).



Protocole HbbTV et sécurité : quelques expérimentations

Yann Bachy, Vincent Nicomette, Eric Alata, Mohamed Kaâniche,
Jean-Christophe Courrège et Pierre Lukjanenko

SSTIC 2015