L'analyse de vulnérabilités : les systèmes embarqués critiques et les objets grand public connectés à Internet

Eric Alata - Mohamed Kâaniche - Vincent Nicomette

INSA - LAAS/CNRS

Séminaire sur la Confiance Numérique - 07 Avril 2016

Sécurité des systèmes informatiques (1/2)

Etat des lieux

- Envisager la sécurité des systèmes informatiques aujourd'hui ne se limite pas aux PCs de bureau et aux serveurs
- L'informatique est partout
  - $\Rightarrow$ Tous les moyens de transports (avions, voiture, etc)
  - $\Rightarrow$ Tous les objets connectés de notre quotidien (téléphones, systèmes d'alarmes, fridigaires, compteurs, systèmes de santé, Smart TV, etc)
- Tous ces systèmes utilisent des moyens de communications très variés, filaires et non filaires, supportés par de multiples technologies
- La sécurité des ces "nouveaux systèmes informatiques" est-elle réellement considérée sérieusement ?

Sécurité des systèmes informatiques (2/2)

Travaux du LAAS

- L'équipe TSF s'intéresse depuis toujours à la sécurité des systèmes informatiques
- Depuis quelques années, focalisation sur les couches basses du logiciel, en interaction avec le matériel
  $\Rightarrow$ deux thèses soutenues et une en cours
- Depuis quelques années, diversification de nos travaux vers ces "nouveaux systèmes informatiques", en particulier :
  - Sécurité des systèmes embarqués avioniques (étude en collaboration avec Airbus)
  - Sécurité des communications dans les véhicules (étude en collaboration avec Renault)
  - Sécurité des équipements grand public connectés à Internet (étude en collaboration avec Thalès) : nos premiers "objets connectés"
  - $\Rightarrow$ trois thèses soutenues

Pourquoi la recherche de vulnérabilités ? (1/2)

Méthodes de défense

- Méthodes formelles pour la spécification, le développement et la vérification (ISO/IEC 15408 Common Criteria notamment)
- Mécanismes et outils de protection : pare-feux, réseaux privés, détection d'intrusion, authentification, contrôle d'accès, etc.
- La recherche de vulnérabilités et la proposition de contre-mesures

Pourquoi la recherche de vulnérabilités ? (2/2)

Limites des méthodes formelles

- Difficulté d'exprimer des propriétés de haut niveau (confidentialité, intégrité et confidentialité) et l'implémentation de mécanismes subtiles (gestion des modes d'exécution, des caches, des interruptions, etc)
- Difficulté de modéliser un noyau complet, non trivial : les certifications EAL6 ou 7 ne concernent que des noyaux minimalistes
- Une version précise est certifiée et le processus est long ; pendant ce temps, le développement continue $\rightarrow$ on recertifie ?

Logiciels certifiés font des suppositions sur le matériel

- Sibert et. al 95 : deux logiciels certifiés A1 dans les années 90
  - Tous ces logiciels ont été implémentés sur architecture x86 (en particulier 80386)
  - Dans le même temps, vulnérabilités découvertes sur ce type de processeurs.

Sécurité des noyaux de systèmes embarqués

Systèmes avioniques (2010-2014)

Thèse de d'Anthony Dessiatnikoff

Projet ANR SOBAS

Contexte des travaux (1/2)

Les systèmes avioniques d'aujourd'hui : l'IMA

- Evolution des systèmes embarqués dans des avions vers une architecture de type IMA (*Integrated Modular Avionics*)
  - Fin de l'isolation complète des fonctions avioniques
  - Partage de ressources et communications via un bus (AFDX)
  - Utilisation de COTS
- Jusqu'à peu, beaucoup de normes concernant la safety mais peu concernant la security $\Rightarrow$ cela change aujourd'hui, les malveillances sont sérieusement considérées

Contexte des travaux (2/2)

Le projet SOBAS

- Projet ANR *Securing On-Board Aerospace Systems*
- Objectif : étudier les vulnérabilités des couches basses du logiciel
- En pratique : étude d'un noyau embarqué expérimental fourni par Airbus France avec ses sources
  - Réalisation d'un certain nombre d'expérimentations visant à mettre en évidence des vulnérabilités
  - Ces expérimentations peuvent influer sur le développement du noyau (qui est en cours) : un des objectifs de SOBAS

Le système embarqué étudié

Caractéristiques

- Un noyau minimaliste
- Des partitions utilisateurs, avec un faible niveau de criticité
- Des partitions système, avec un haut niveau de criticité
- Partitionnement spatial et temporel assuré par la MMU (*Memory Management Unit*) et le MPIC (*Multicore Programmable Interrupt Controller*)

La plateforme de tests

Caractéristiques

- Plateforme P4080 de FreeScale
  - Plateforme puissante : nombreuses interfaces réseaux, accéleration matérielle du traitement et du chiffrement des communications
  - 8 coeurs, MMU, caches, PAMU (équivalent IOMMU)
- CodeWarrior et un port JTAG : observation et injections d'attaques

t

Expérimentations

Hypothèses d'attaques et catégories d'attaques

- Hypothèse d'attaque : une partition utilisateur non-critique est malveillante et essaie de corrompre une autre partition ou le noyau lui-même

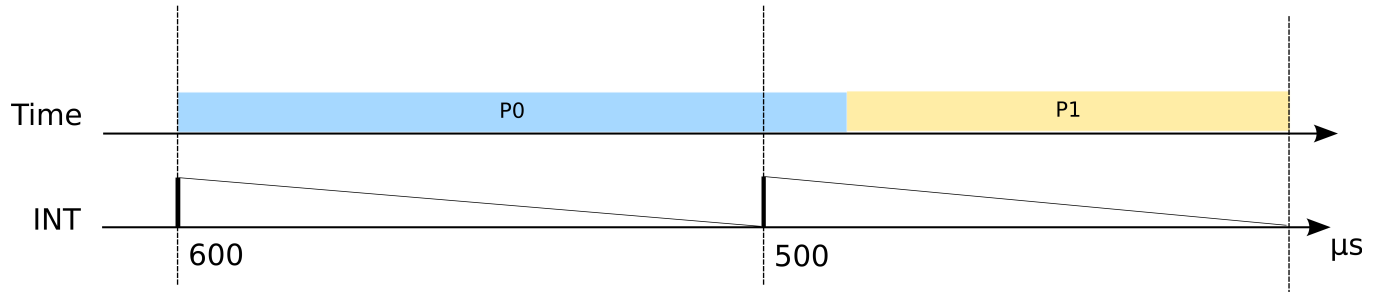
Attaques réalisées

- Attaques ciblant les fonctions de base d'un calculateur (processeur, gestion de la mémoire, gestion du temps, etc)
- Attaques ciblant les mécanismes de tolérance aux fautes (diagnostic de fautes)

Exemple d'attaque (1/2)

Gestion du temps

- Objectif de l'attaque : modifier le temps de cycle d'une partition critique depuis une partition non-critique
- Le scheduling des partitions est fait grâce au MPIC : impossible de générer des interruptions depuis une partition utilisateur
- Idée : augmenter la durée d'exécution de la partition malveillante pour réduire la durée d'exécution de la partition critique schédulée juste après
  1. Réaliser une boucle jusqu'à la fin de la durée d'exécution "normale"
  2. Déclencher une exception de façon à exécuter du code noyau non interruptible, le plus long possible



Exemple d'attaque (2/2)

Diagnostic de fautes

- Mise à l'épreuve de la gestion des exceptions à l'aide d'un programme de type `crashme`
- Programme exécuté sur 1 million de cycles de la partition : exécution de 100 instructions aléatoires à chaque cycle
- Pas de crash du noyau mais ...
  - Beaucoup d'exceptions provoquent à tord le redémarrage de la partition, du noyau ou du système complet
    $\Rightarrow$ Nécessité d'améliorer l'analyse des causes d'exceptions pour prendre des décisions moins radicales

Sécurité des équipements grand public connectés à Internet

Systèmes grand public (2012-2015)

Thèse de de Yann Bachy
Thèse CIFRE Thalès

Émergence des équipements grand public connectés

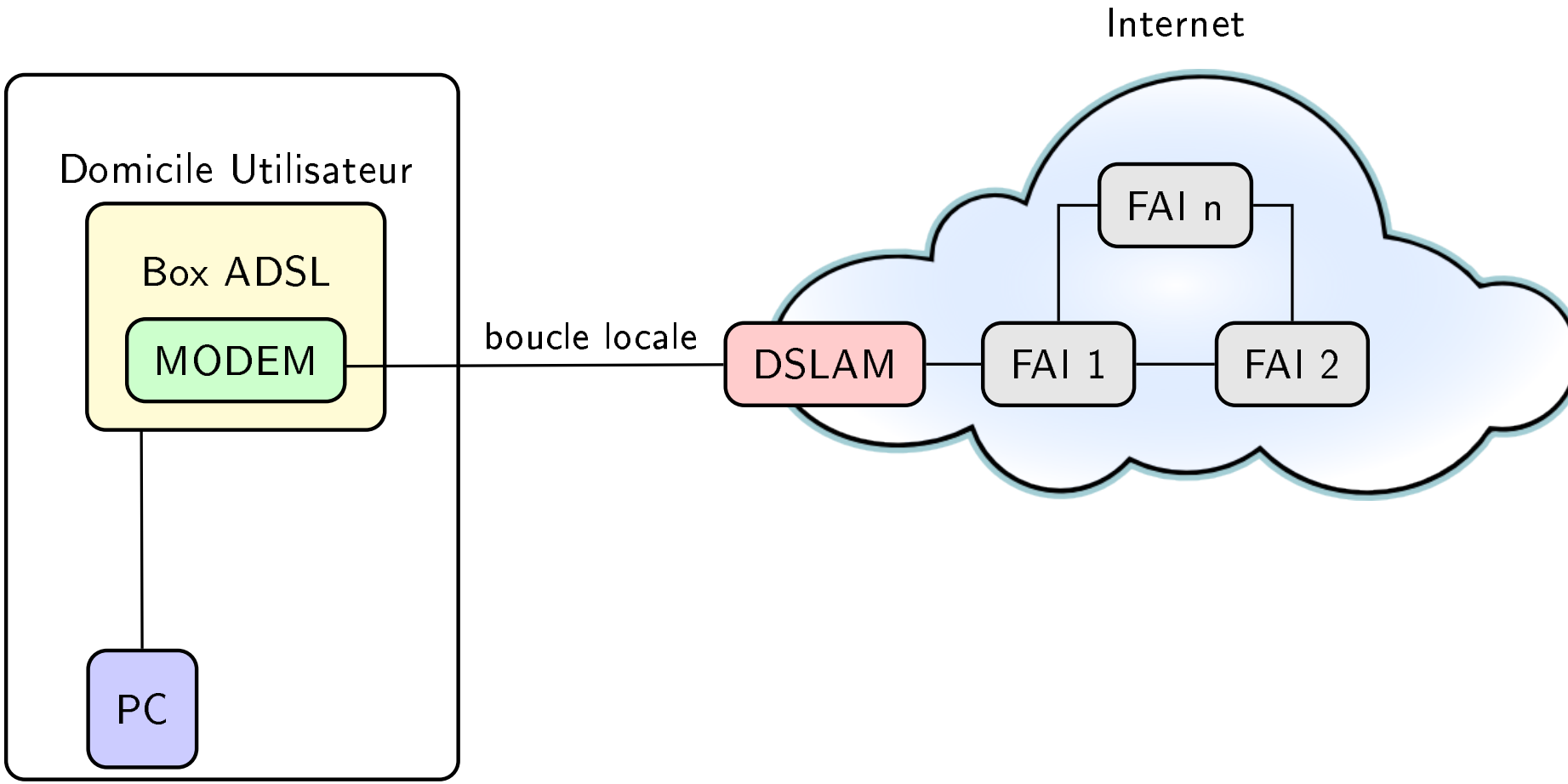
Les risques ?

- Pas de réelle prise en compte de la sécurité ni de la protection de la vie privée par les constructeurs de ces matériels
- Cible de notre étude : équipements connectés possédant plusieurs interfaces de communication, pouvant être utilisés comme relai dans le cas d'attaque
  - 2 cas d'étude :
    1. Box ADSL : interface LAN, interface WAN vers le fournisseur d'accès Internet (FAI)
    2. TV connectée : interface LAN, interface DVB vers le fournisseur de contenu
  - Hypothèse d'attaque : utiliser la communication avec les fournisseurs de service qui est insufisamment sécurisée

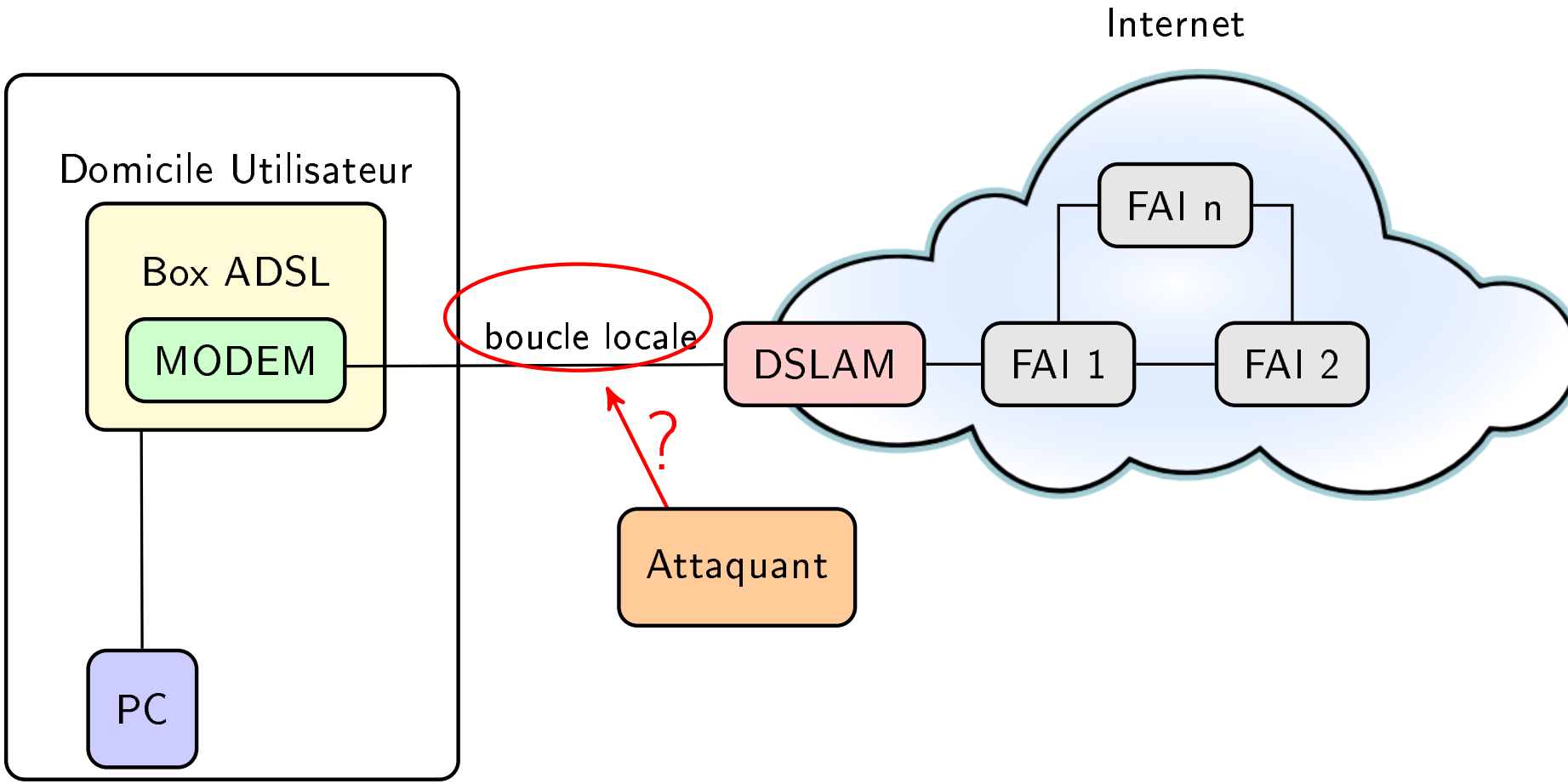
La Box ADSL

- Introduction à la fin des années 90 d'offres Internet "triple play" proposant trois grands axes de services :
  - Web (NAT, DHCP, ...)
  - Télévision (PVR, Replay, ...)
  - Téléphonie (DECT, répondeur, 3G, ...)
- Développement d'équipements, nommés IAD (*Internet Access Device*) ou Box ADSL, permettant de profiter de ces services.
- De plus en plus de services rendant les Box plus riches → augmentation de la surface d'attaque

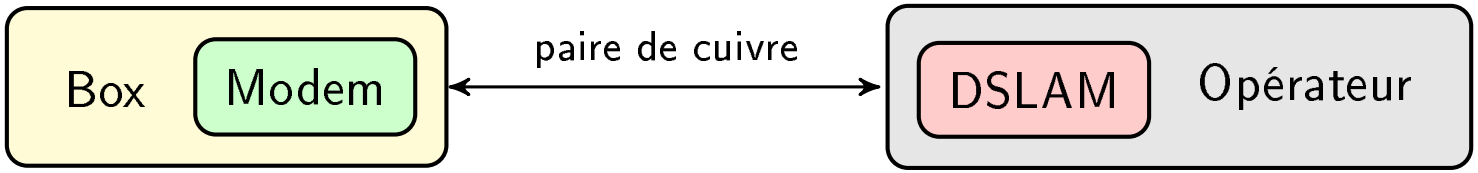
Architecture générale



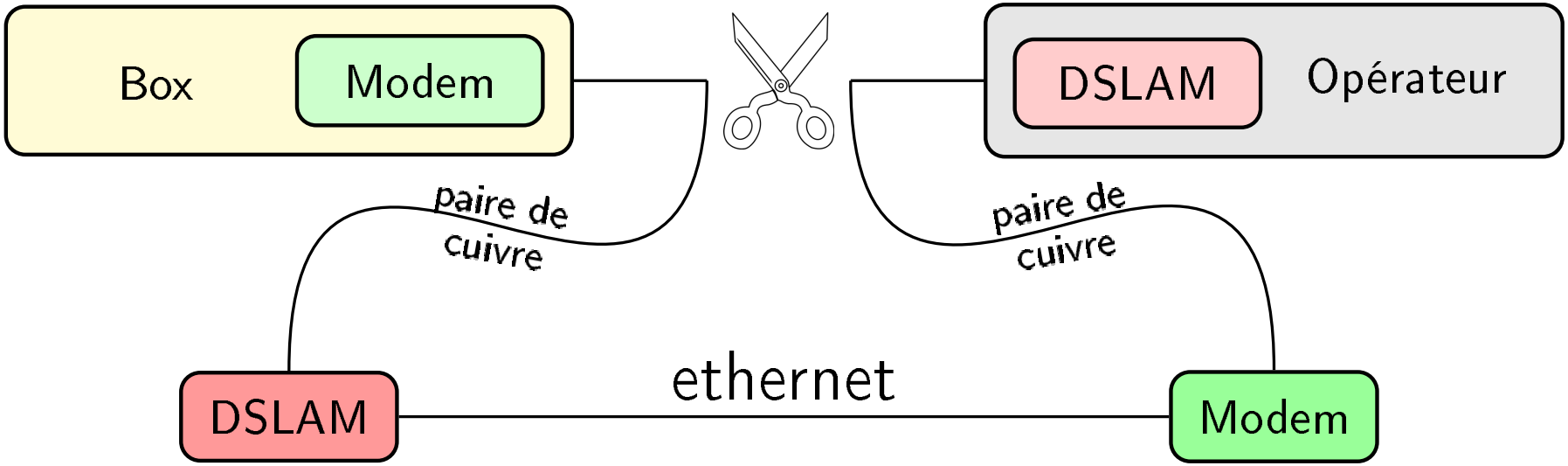
Chemin d'attaque



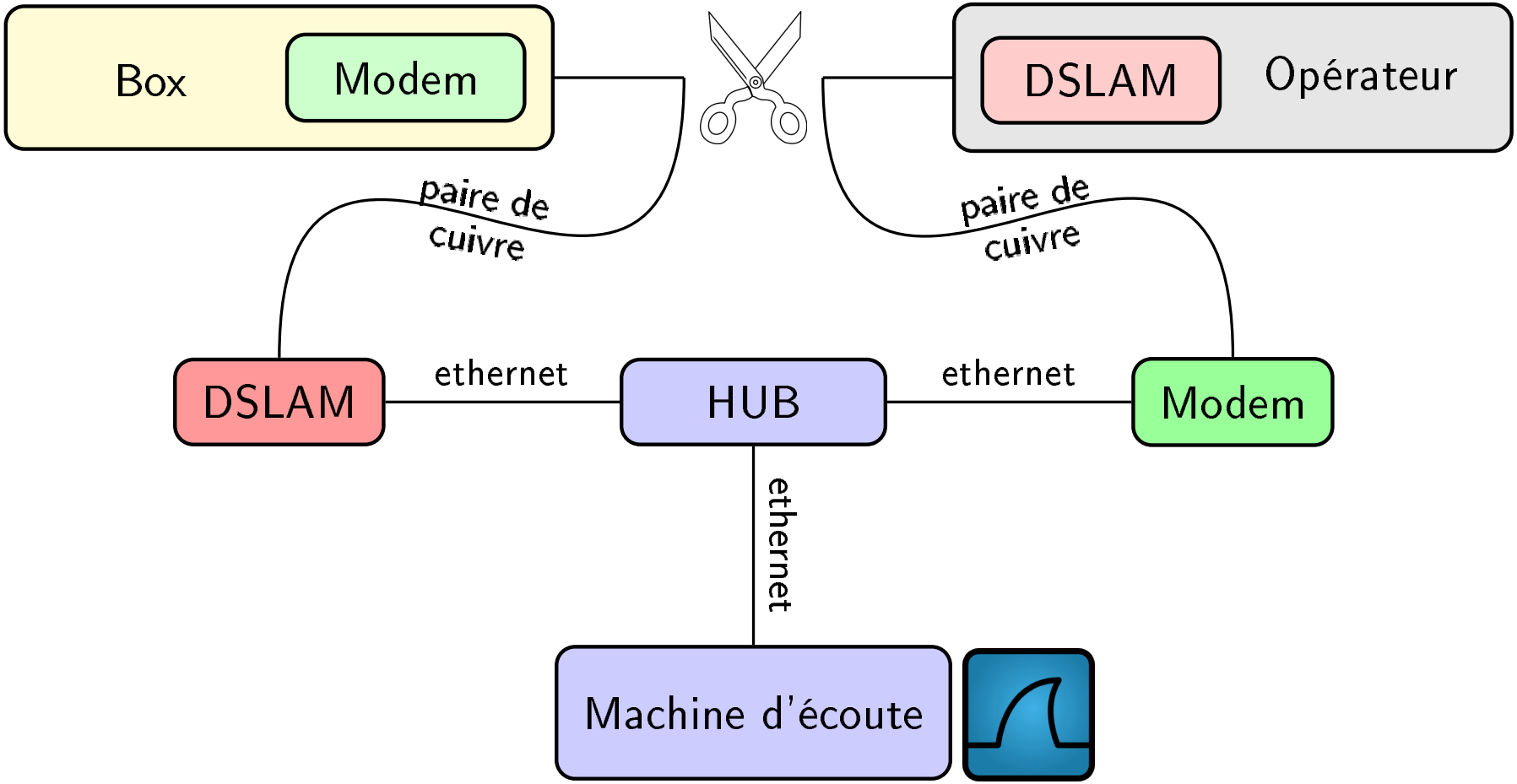
La boucle locale



Observation des communications sur la boucle locale (1/2)



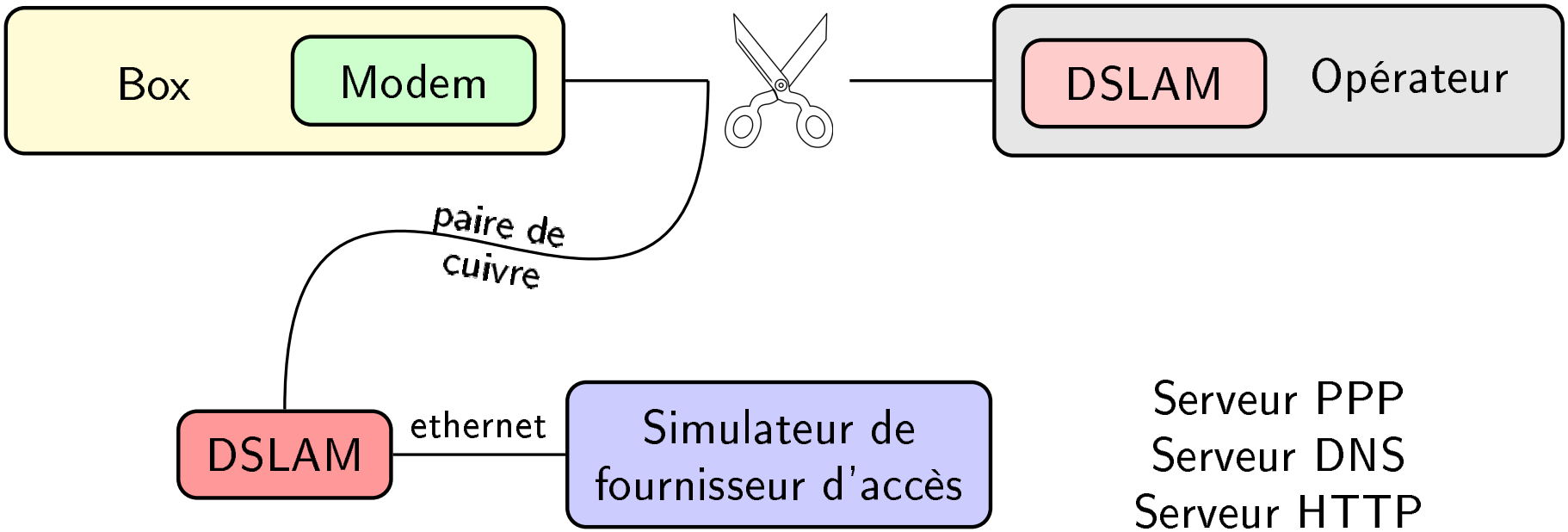
Observation des communications sur la boucle locale (2/2)



Comparaison de plusieurs Box ADSL

Box	ATM	PPP	DHCP	SIP	Configuration	Mise à jour
A	8/35/LLC	chap	no	MD5	HTTP, FTP, SSL	-
B	8/35/LLC	chap	yes	MD5	HTTP, SSL	SSL
C	8/36/VC	no	yes	MD5	SSL	-
D	8/35/LLC	chap	yes	MD5	HTTP	HTTP
E	8/35/LLC	chap	yes	MD5	HTTP	HTTP
F	8/35/LLC	chap	no	MD5	SSL	-

Interruption de la boucle locale et simulation du FAI



Résultats obtenus

Remplacement du firmware

- Désactivation (partielle) du pare-feu
- Ajout d'un compte super-utilisateur
- Désactivation des mises à jour
- Installation de logiciel "soft-phone"

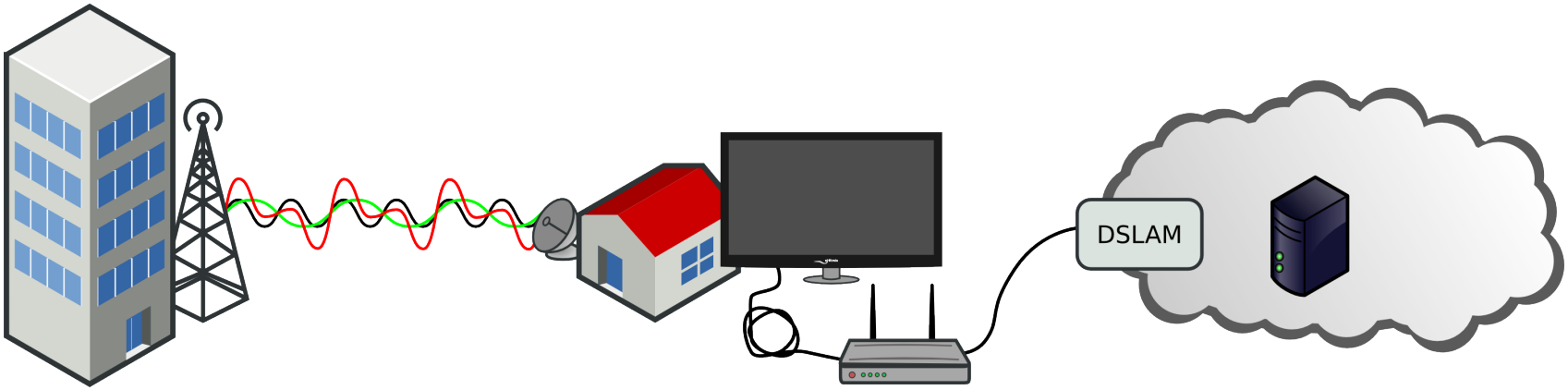
Exploitations réalisées

- Utilisation à distance de la Box pour émettre des appels "surtaxés"
- Connexion à distance sur la Box (via porte dérobée)

Autres exploitations envisagées

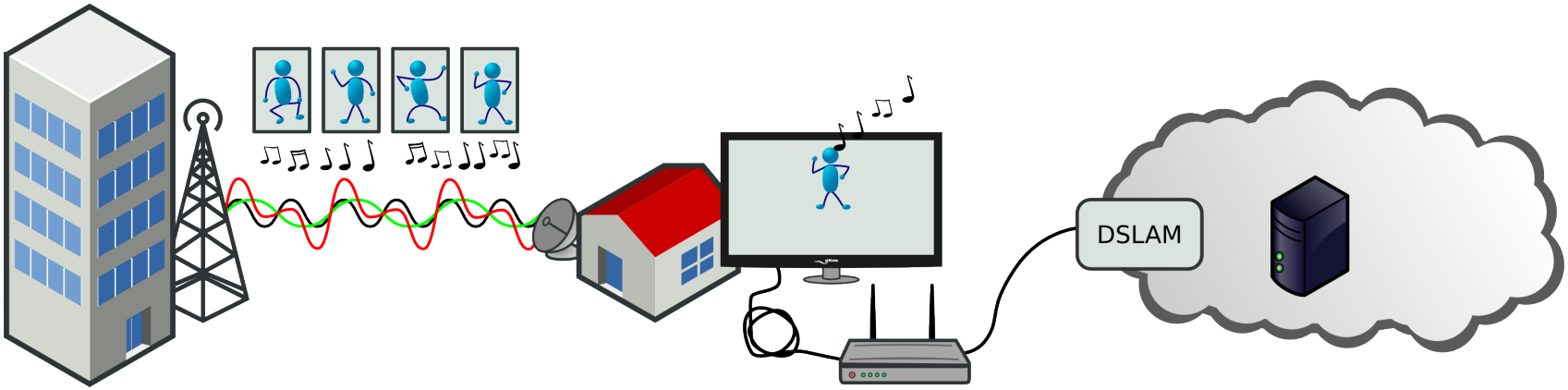
- Réalisation d'un botnet
- Attaques DDos
- Proxy

Utilisation d'une Smart TV



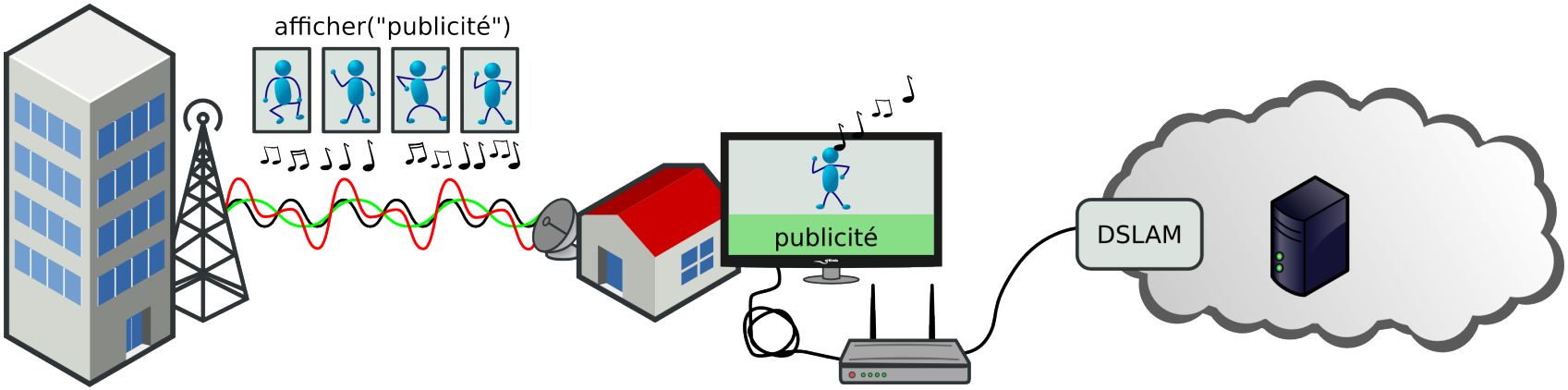
- Envoi d'une séquence vidéo et audio multiplexée
- Ajout d'un flux de données pour contrôler la manière dont le contenu est rendu
  - Affichage d'informations contextuelles (publicité, informations, ...)
  - Interrogation de serveurs distants (vote, sondage, animation, ...)

Utilisation d'une Smart TV



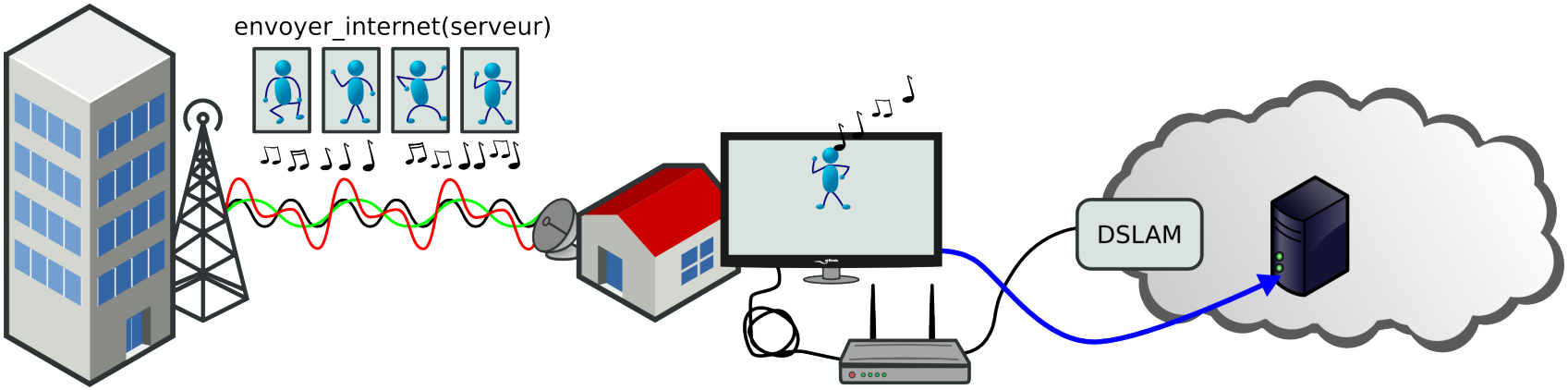
- Envoi d'une séquence vidéo et audio multiplexée
- Ajout d'un flux de données pour contrôler la manière dont le contenu est rendu
  - Affichage d'informations contextuelles (publicité, informations, ...)
  - Interrogation de serveurs distants (vote, sondage, audimat, ...)

Utilisation d'une Smart TV



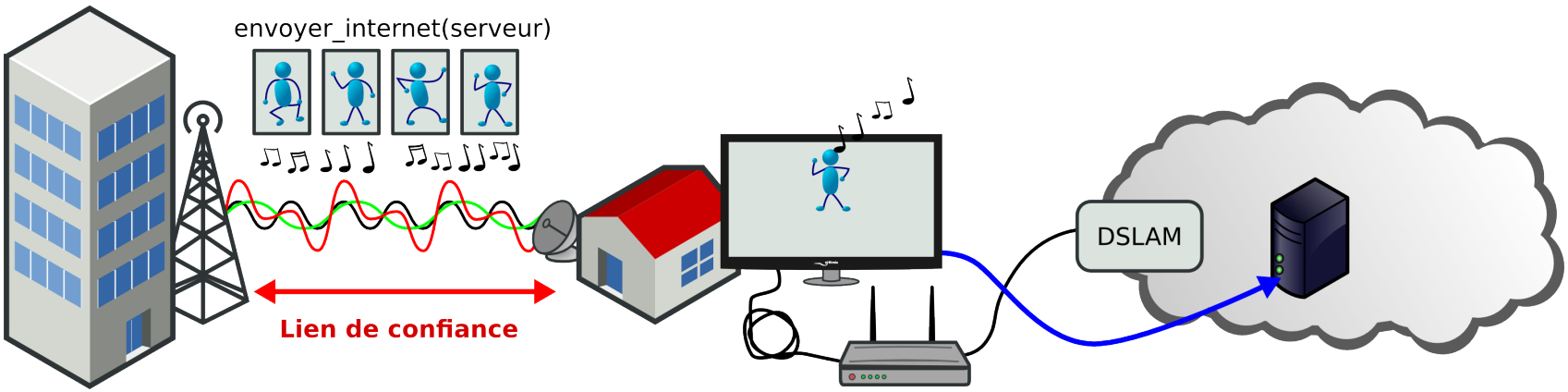
- Envoi d'une séquence vidéo et audio multiplexée
- Ajout d'un flux de données pour contrôler la manière dont le contenu est rendu
  - Affichage d'informations contextuelles (publicité, informations, ...)
  - Interrogation de serveurs distants (vote, sondage, audimat, ...)

Utilisation d'une Smart TV



- Envoi d'une séquence vidéo et audio multiplexée
- Ajout d'un flux de données pour contrôler la manière dont le contenu est rendu
  - Affichage d'informations contextuelles (publicité, informations, ...)
  - Interrogation de serveurs distants (vote, sondage, audimat, ...)

Chemin d'attaque envisagé

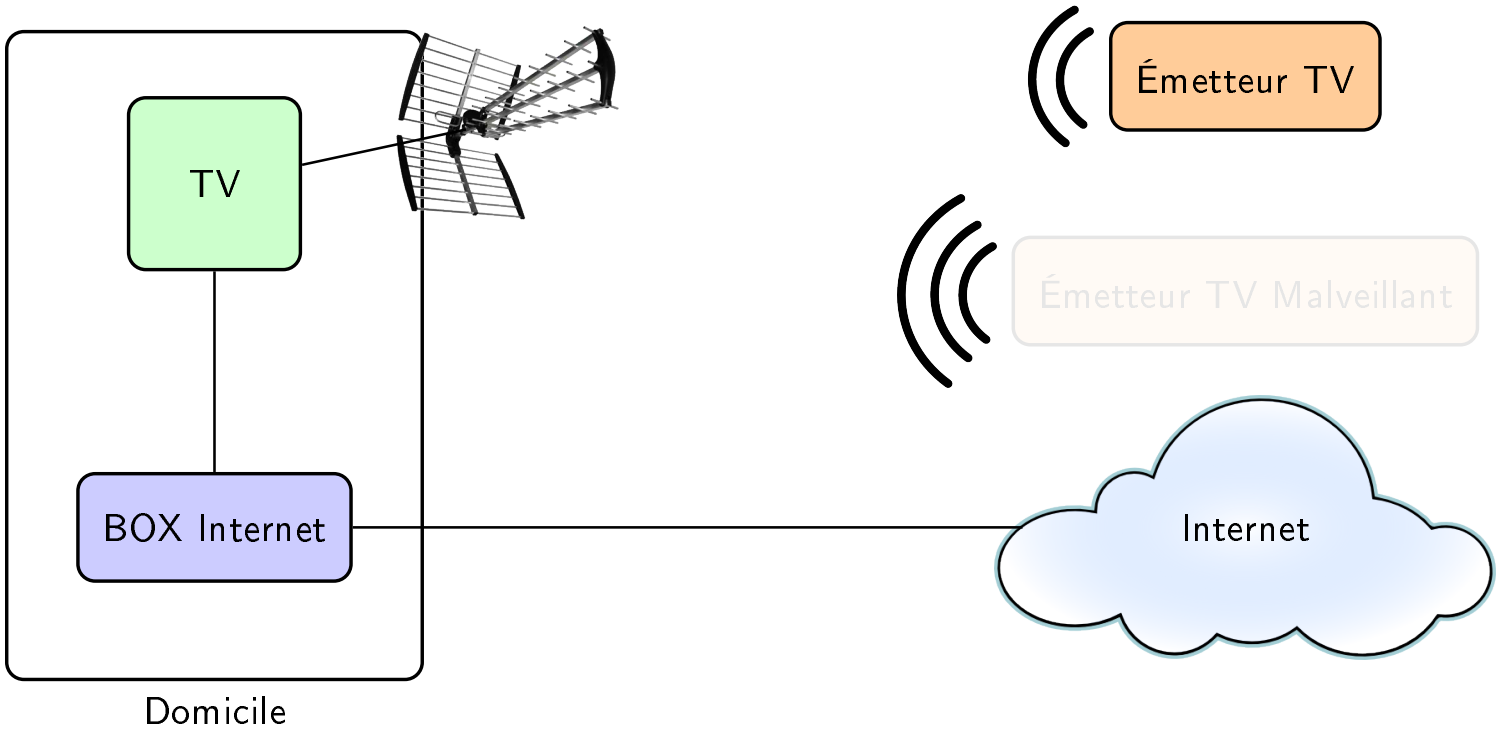


- Lien de confiance de l'antenne vers la TV – confiance légitime ?
- Pas d'authentification du fournisseur de service par la TV

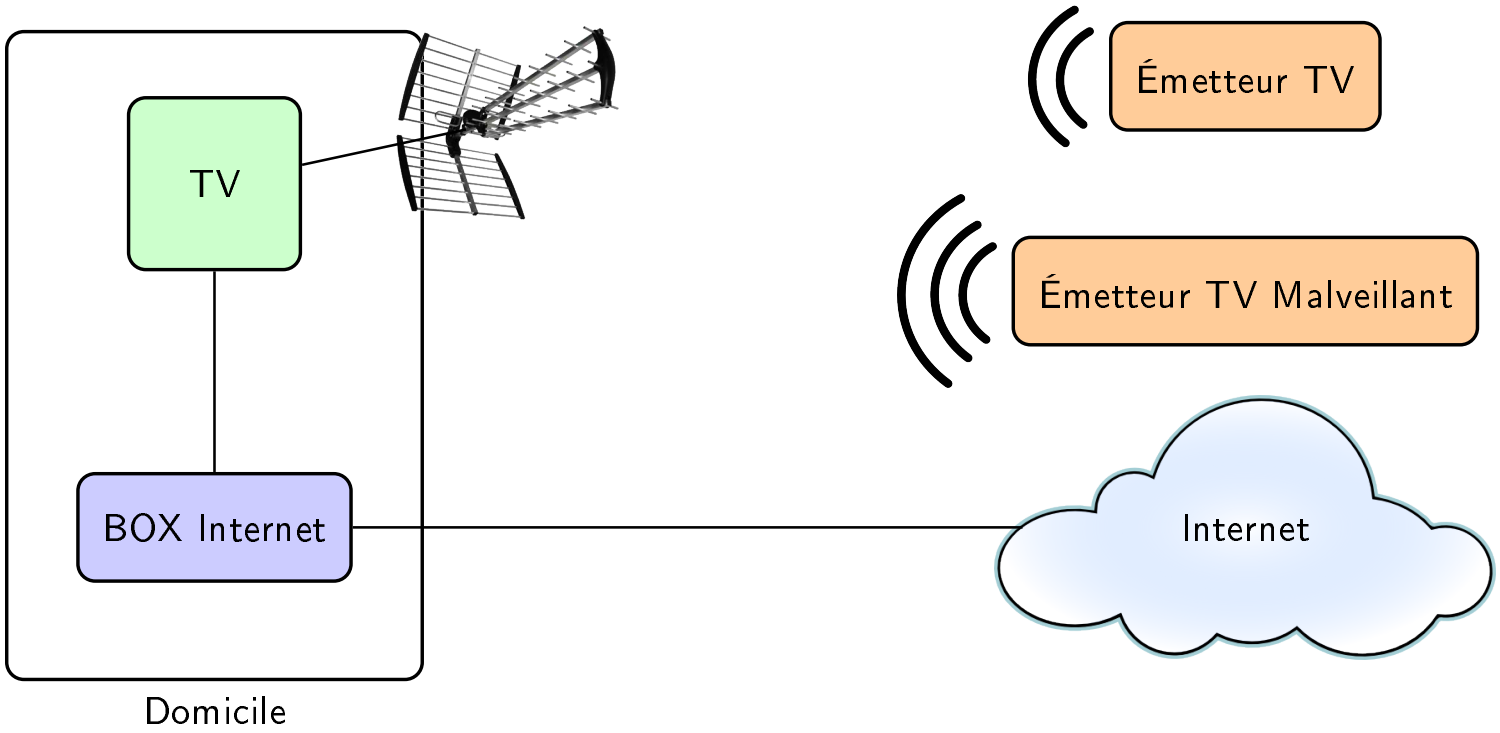
Attaque 1 : Substitution d'une chaîne

- Cette attaque s'applique à tous les téléviseurs (connectés ou non)
- Cette attaque vise à montrer comment l'on peut substituer le contenu (son et image) d'une chaîne.

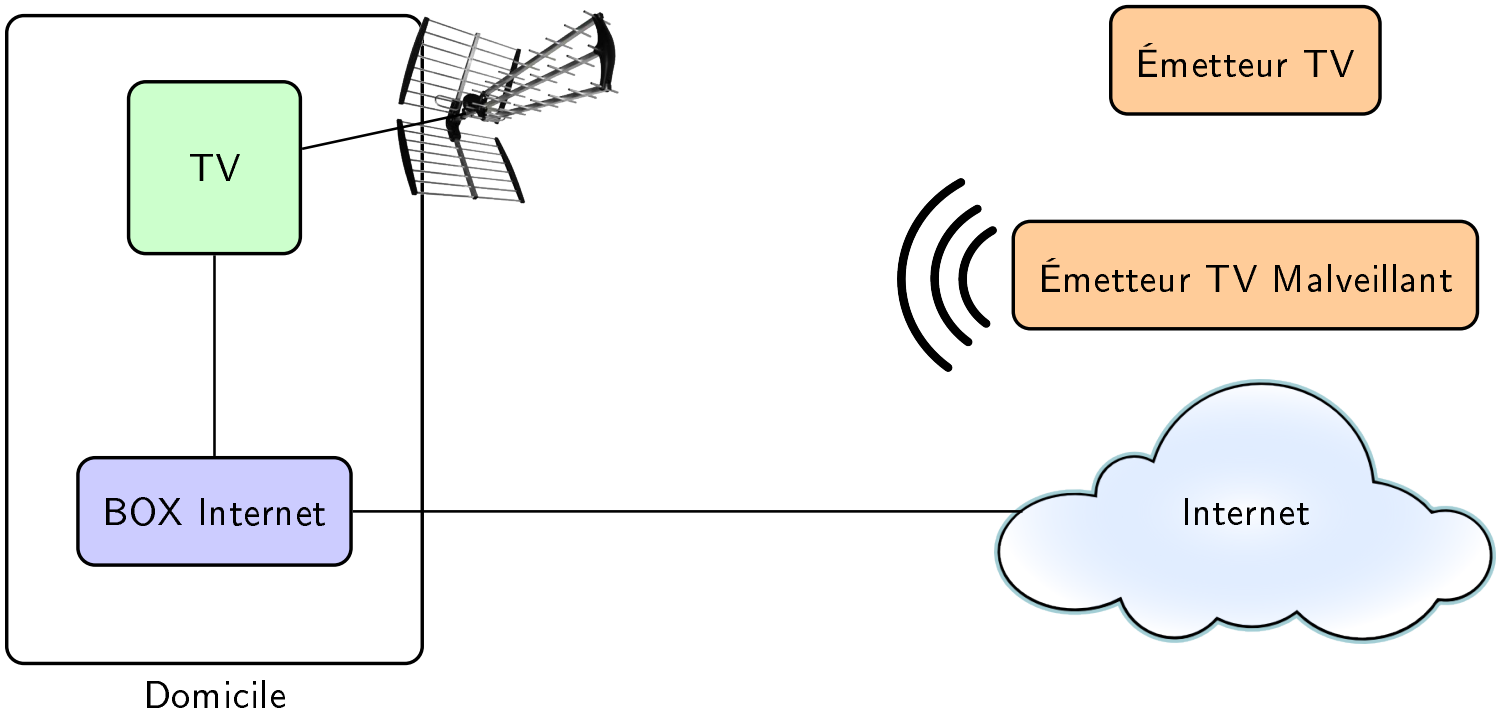
Superposition de signaux



Superposition de signaux



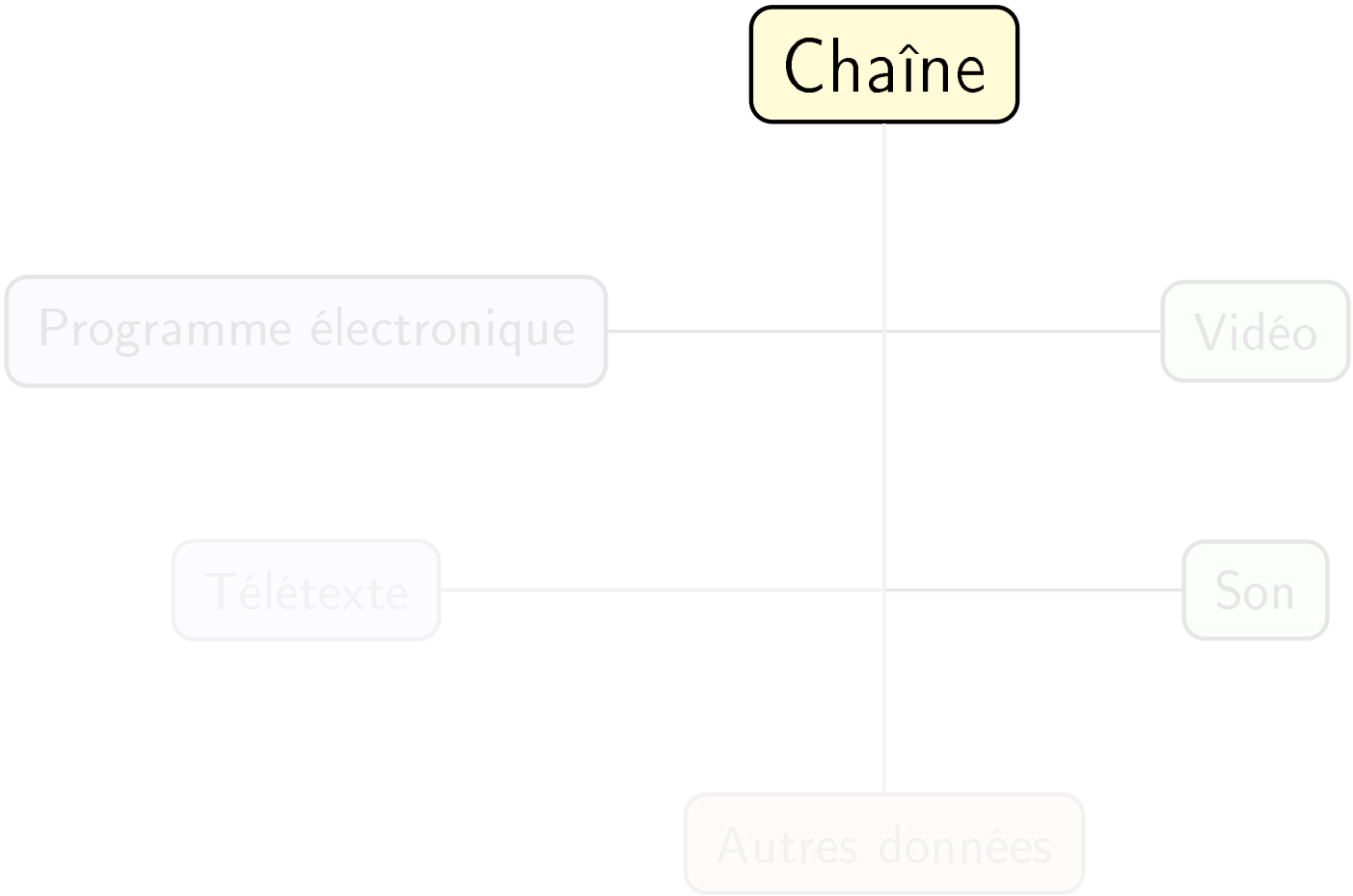
Superposition de signaux



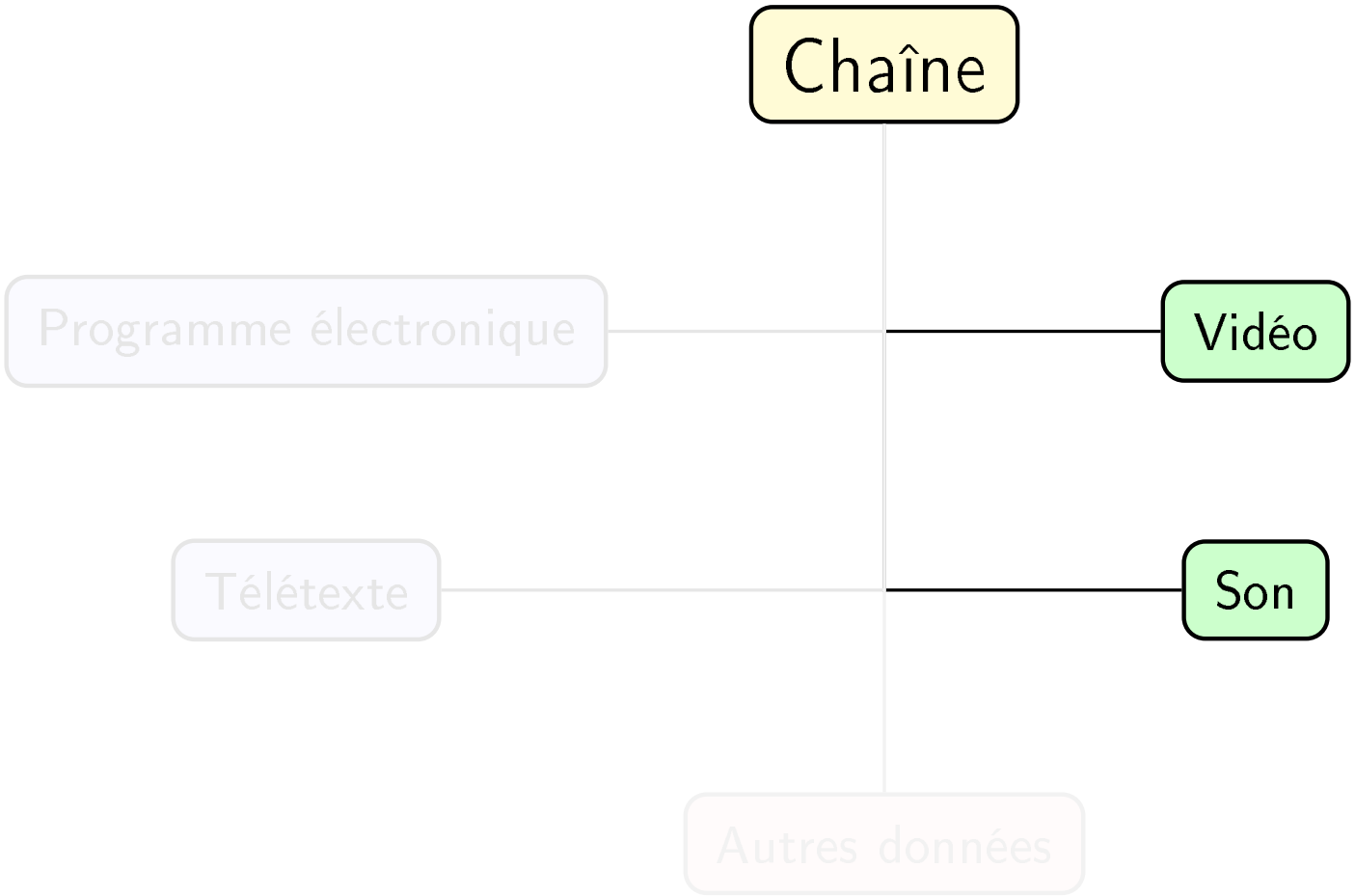
Attaque 2 :
Substitution de données associées à une chaîne

- Cette attaque s'applique uniquement aux téléviseurs connectés.
- Cette attaque vise à mettre en évidence un problème de sécurité des SMART-TV.

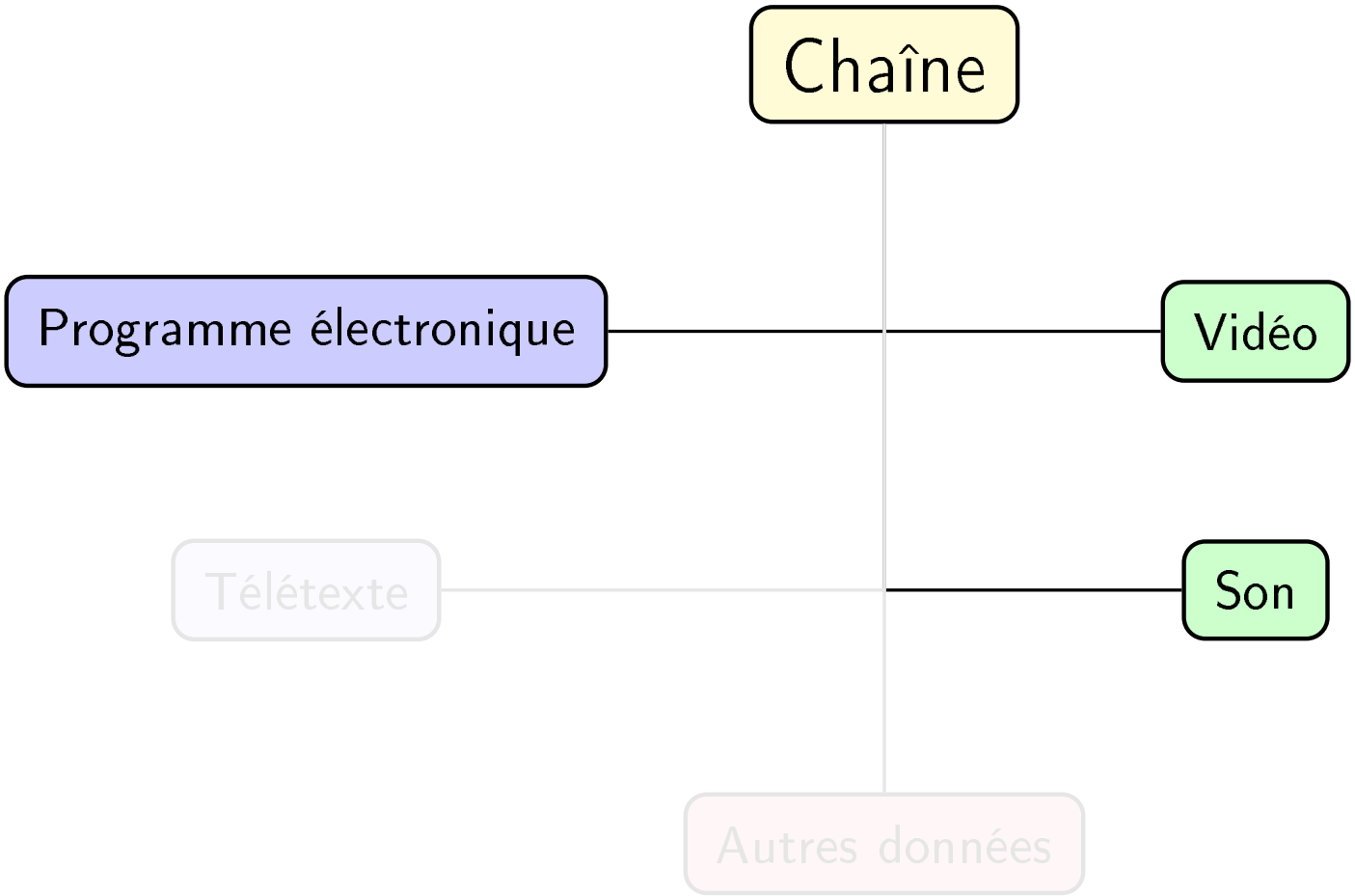
Contenu du signal reçu



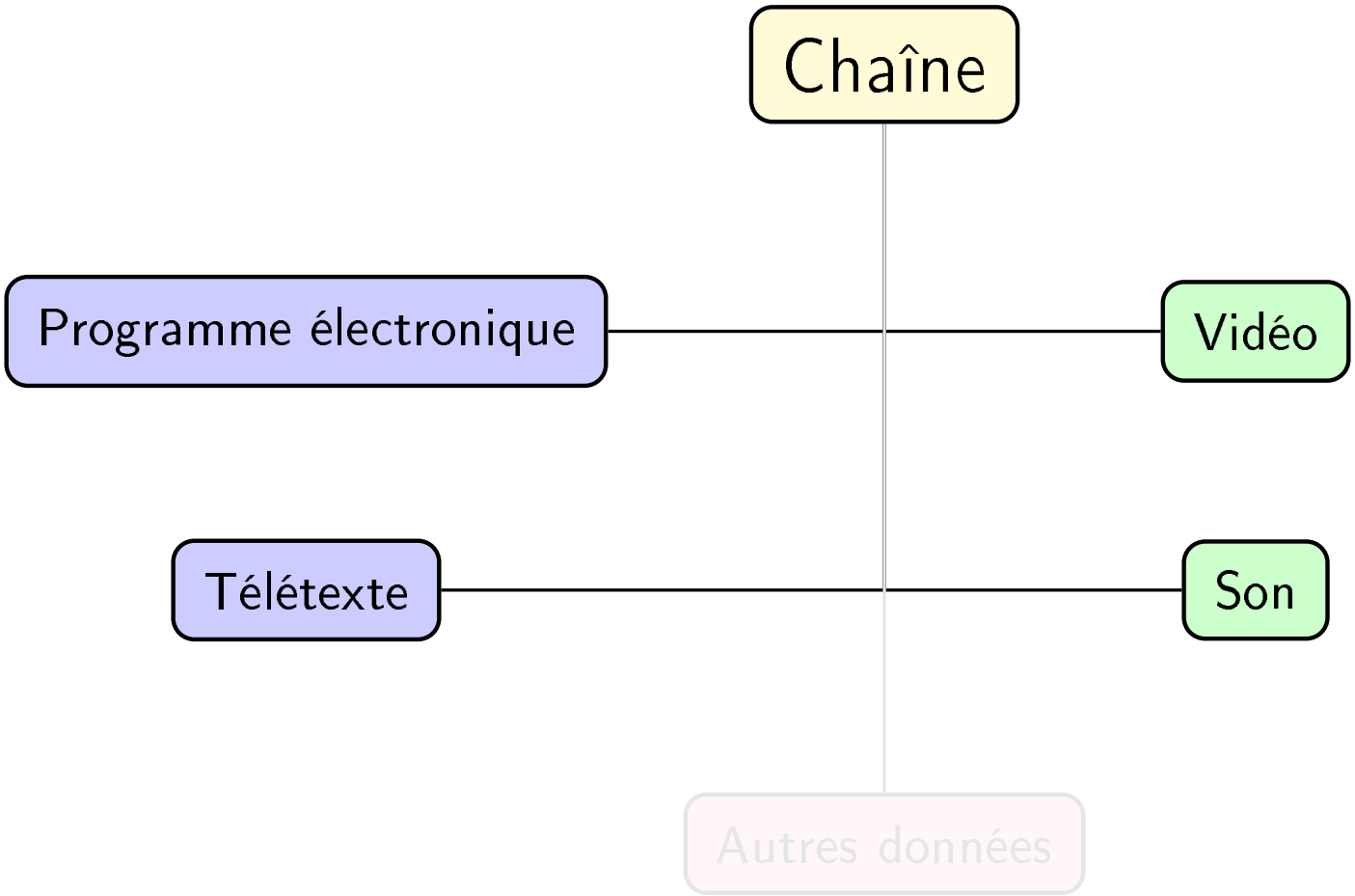
Contenu du signal reçu



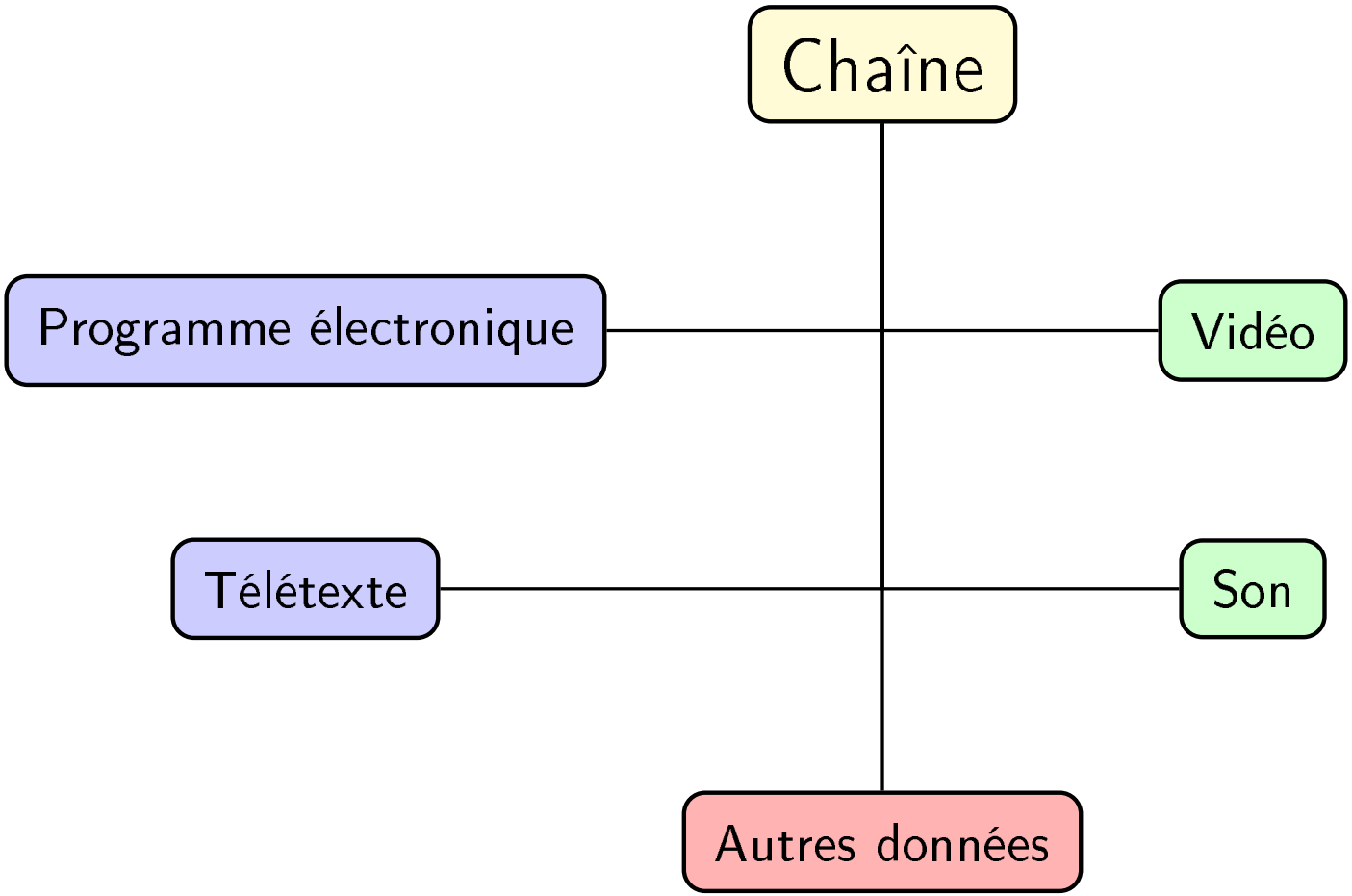
Contenu du signal reçu



Contenu du signal reçu



Contenu du signal reçu

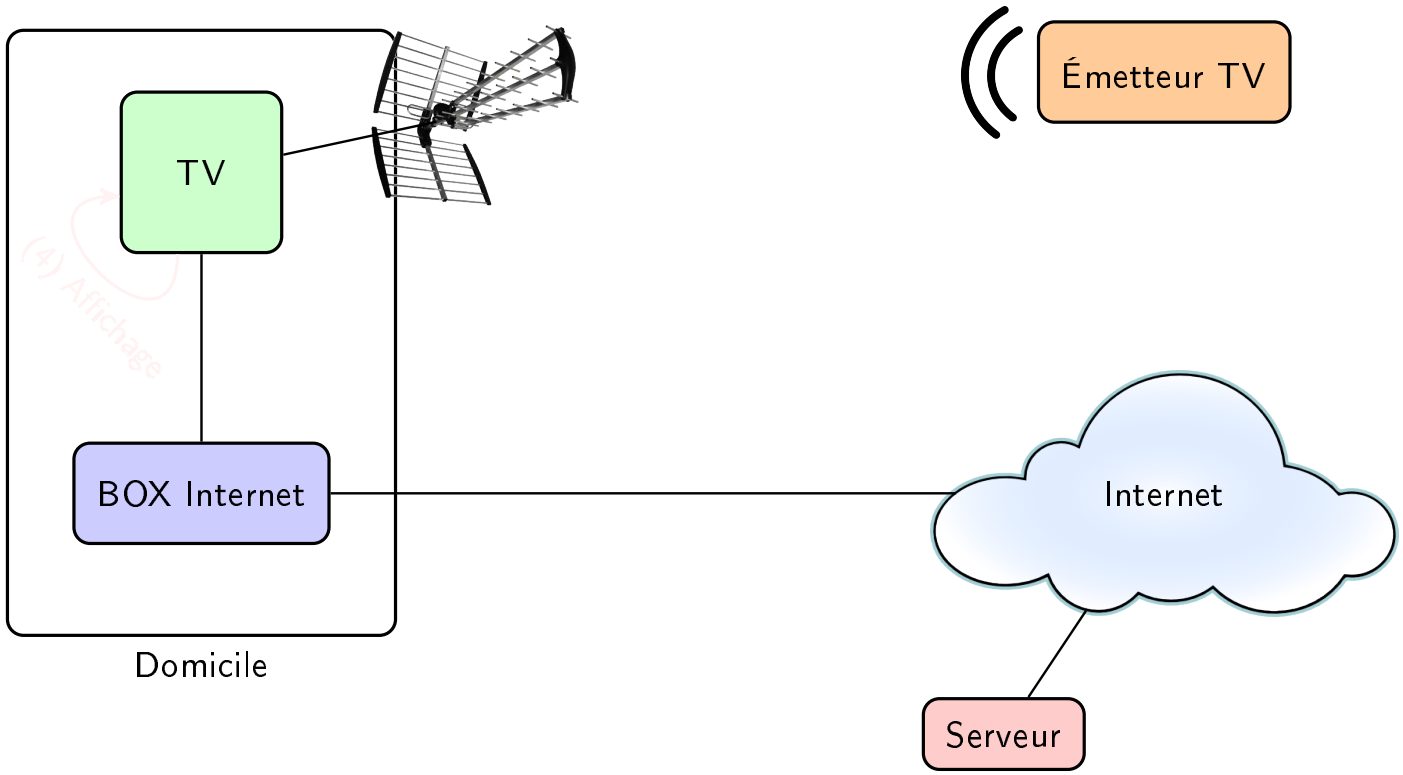


Les "autres données" reçues par le téléviseur

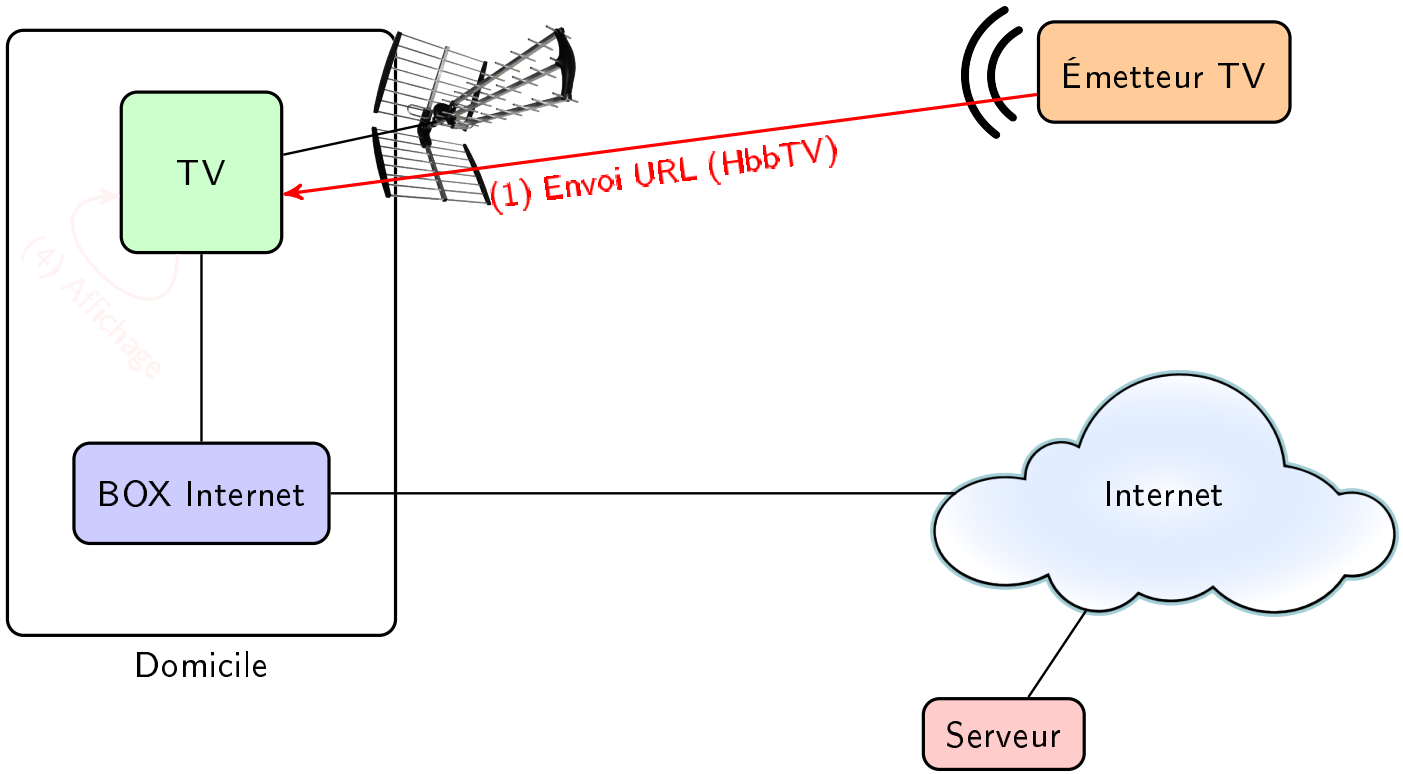
- Informations concernant la chaîne (bouquet, nom, réseau, etc...)
- Informations concernant des "évènements"
- Informations concernant l'heure
- URL de l'**application** associée

Comment fonctionnent ces **applications** ?

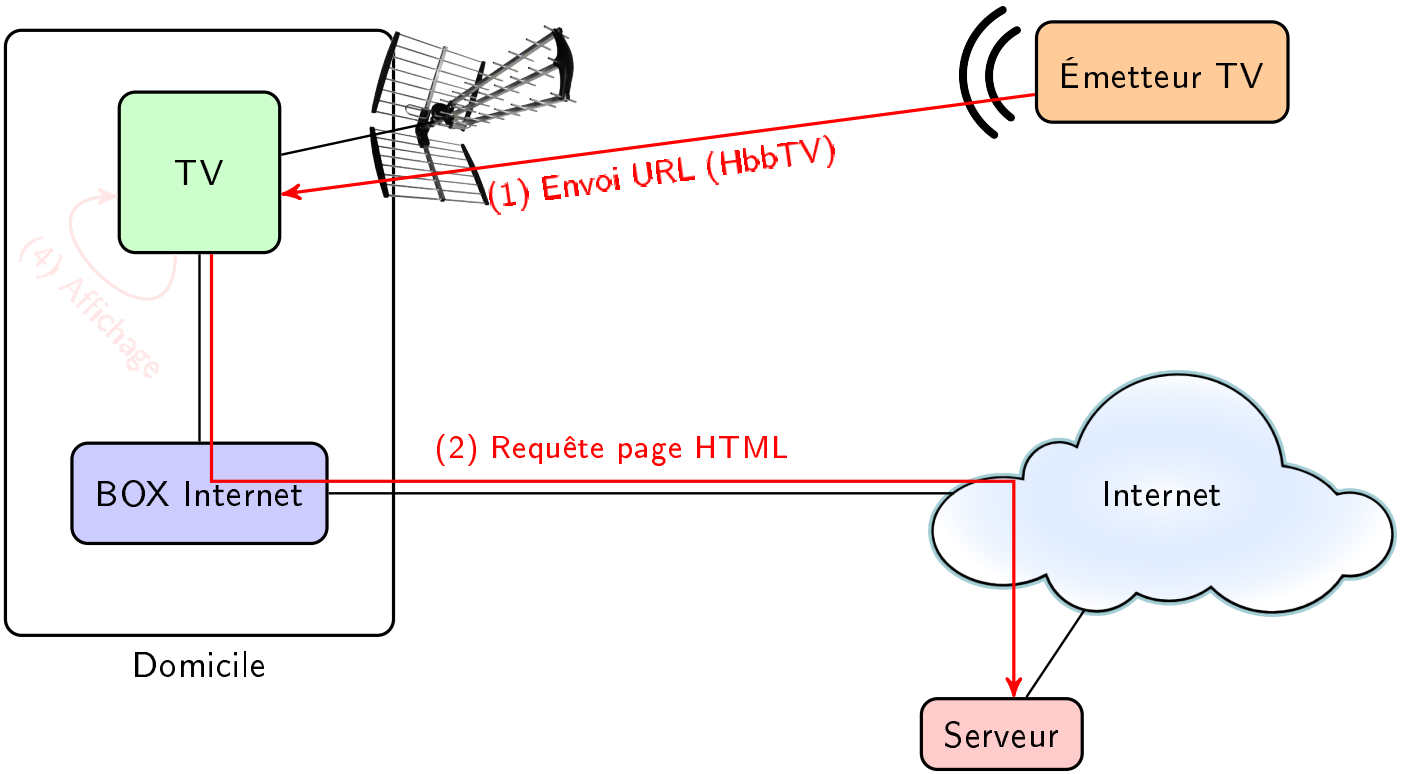
Fonctionnement d'une application



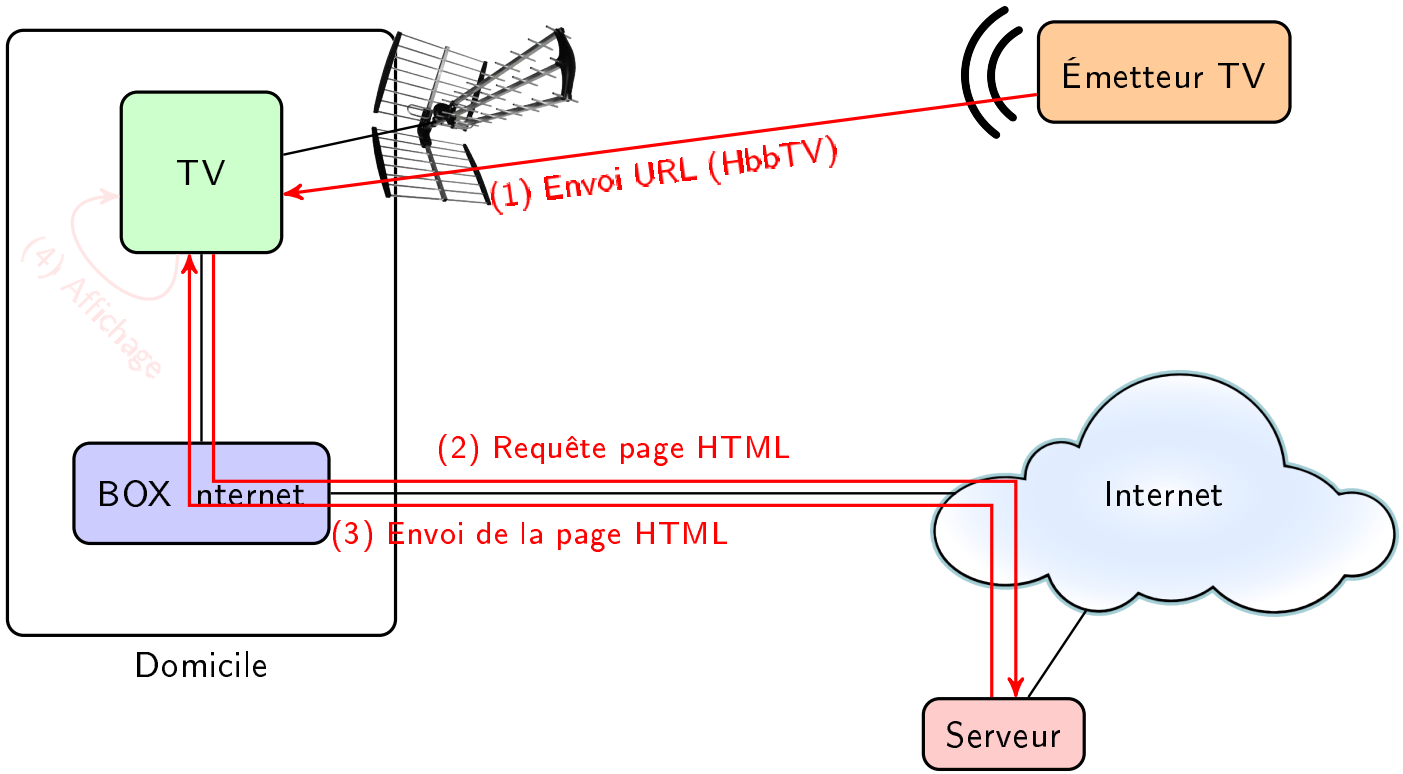
Fonctionnement d'une application



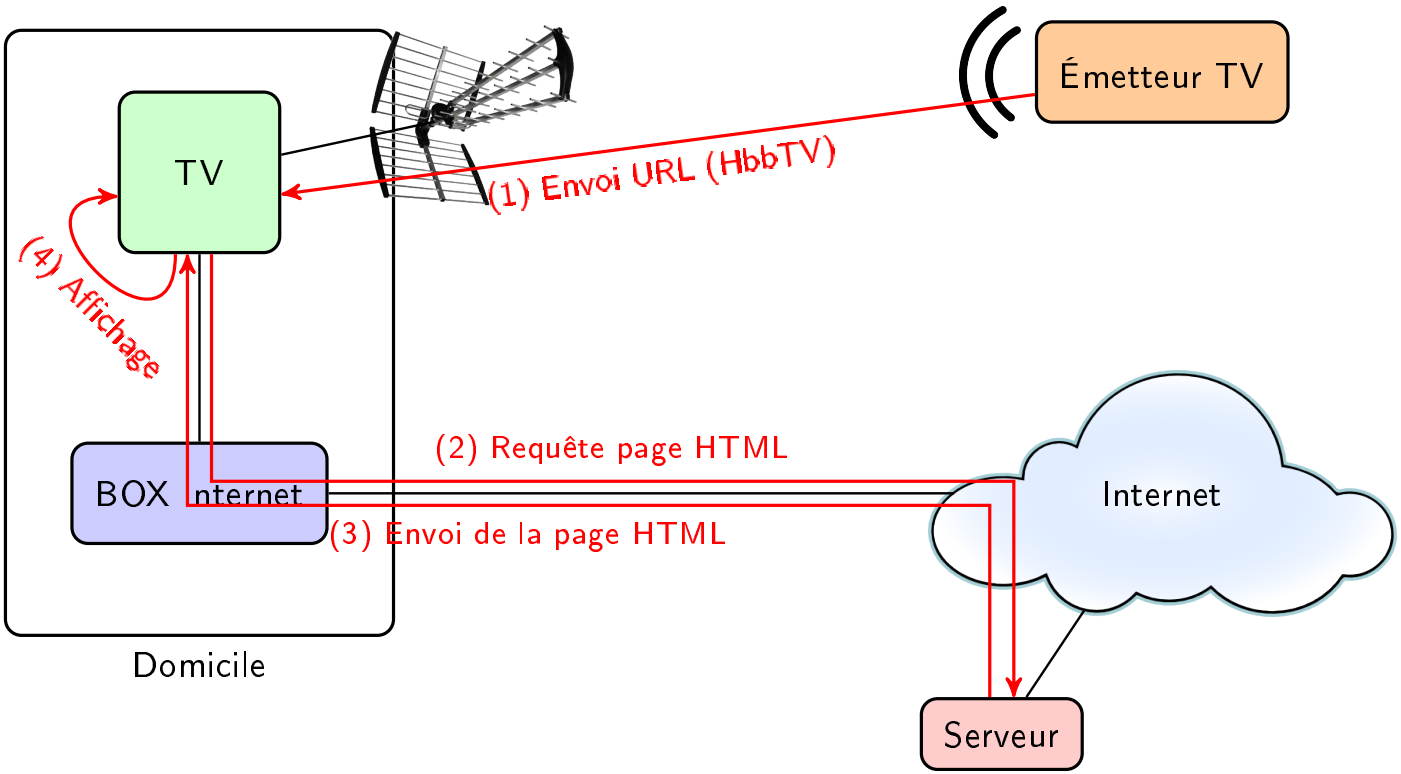
Fonctionnement d'une application



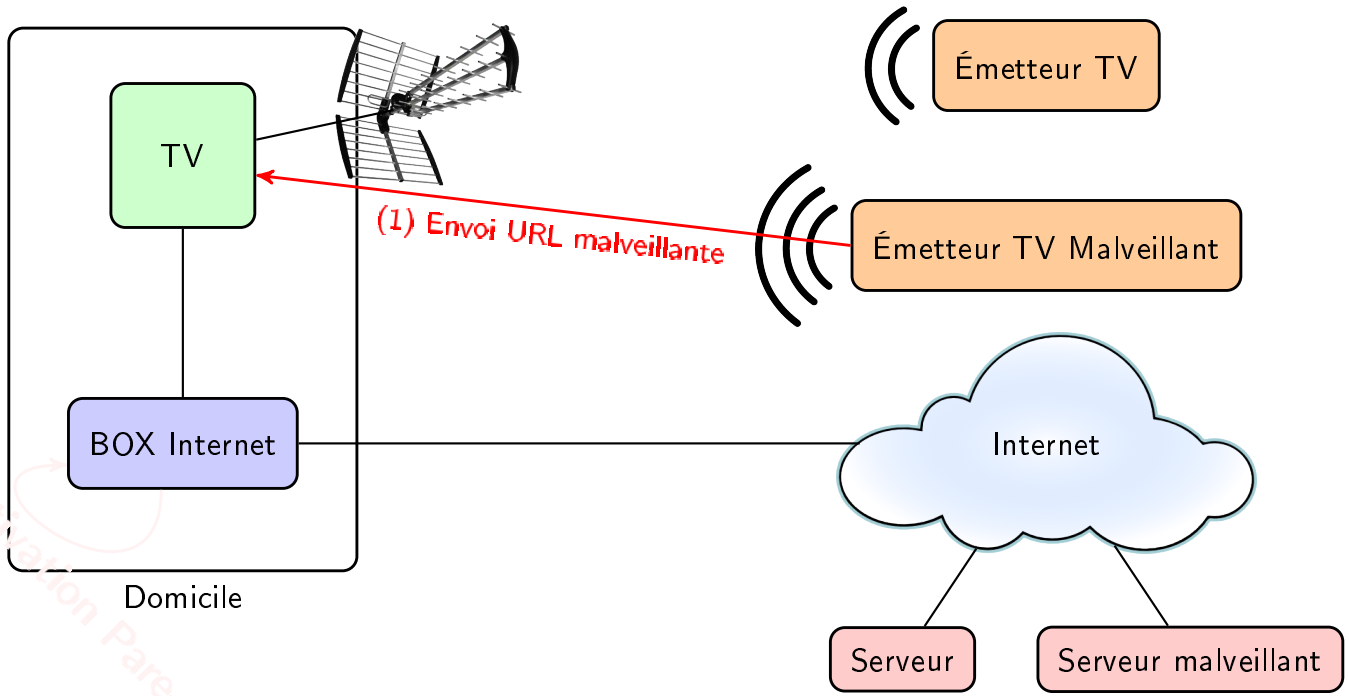
Fonctionnement d'une application



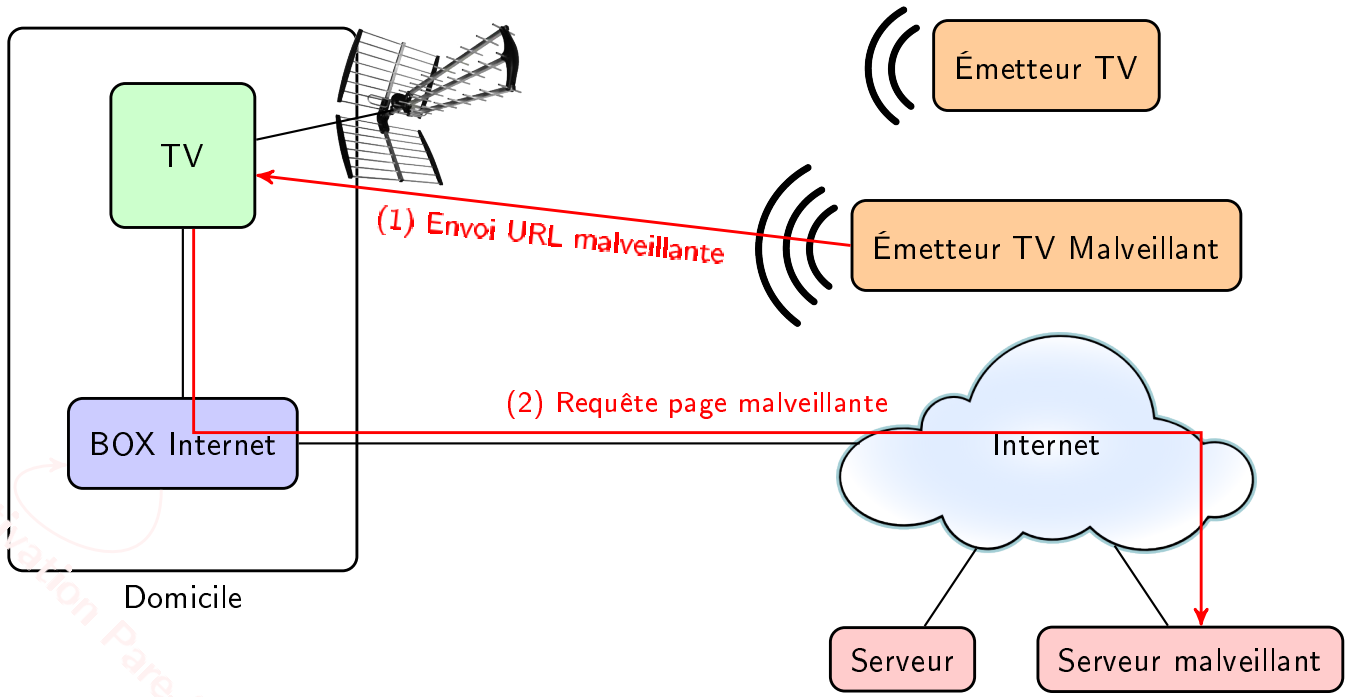
Fonctionnement d'une application



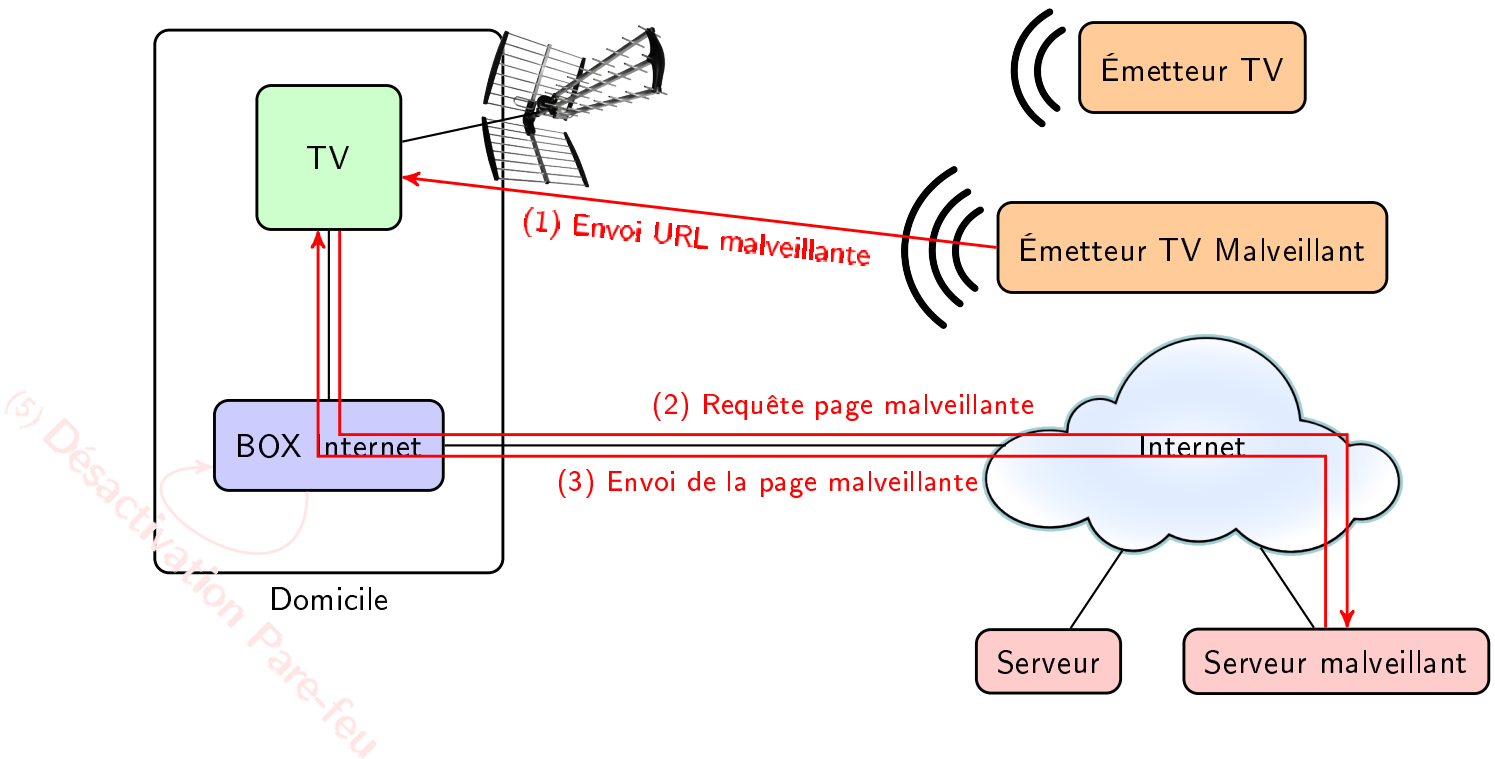
Application Malveillante



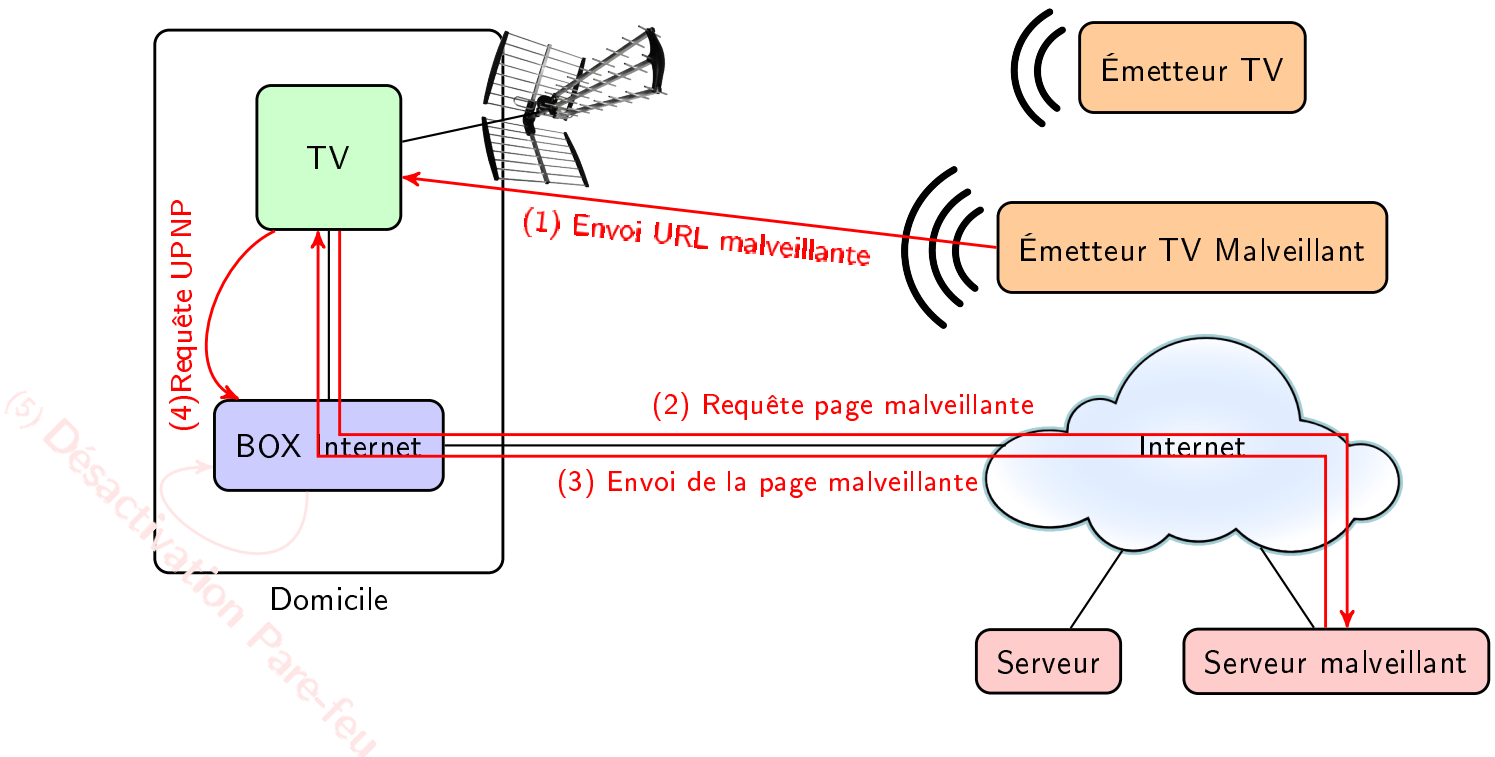
Application Malveillante



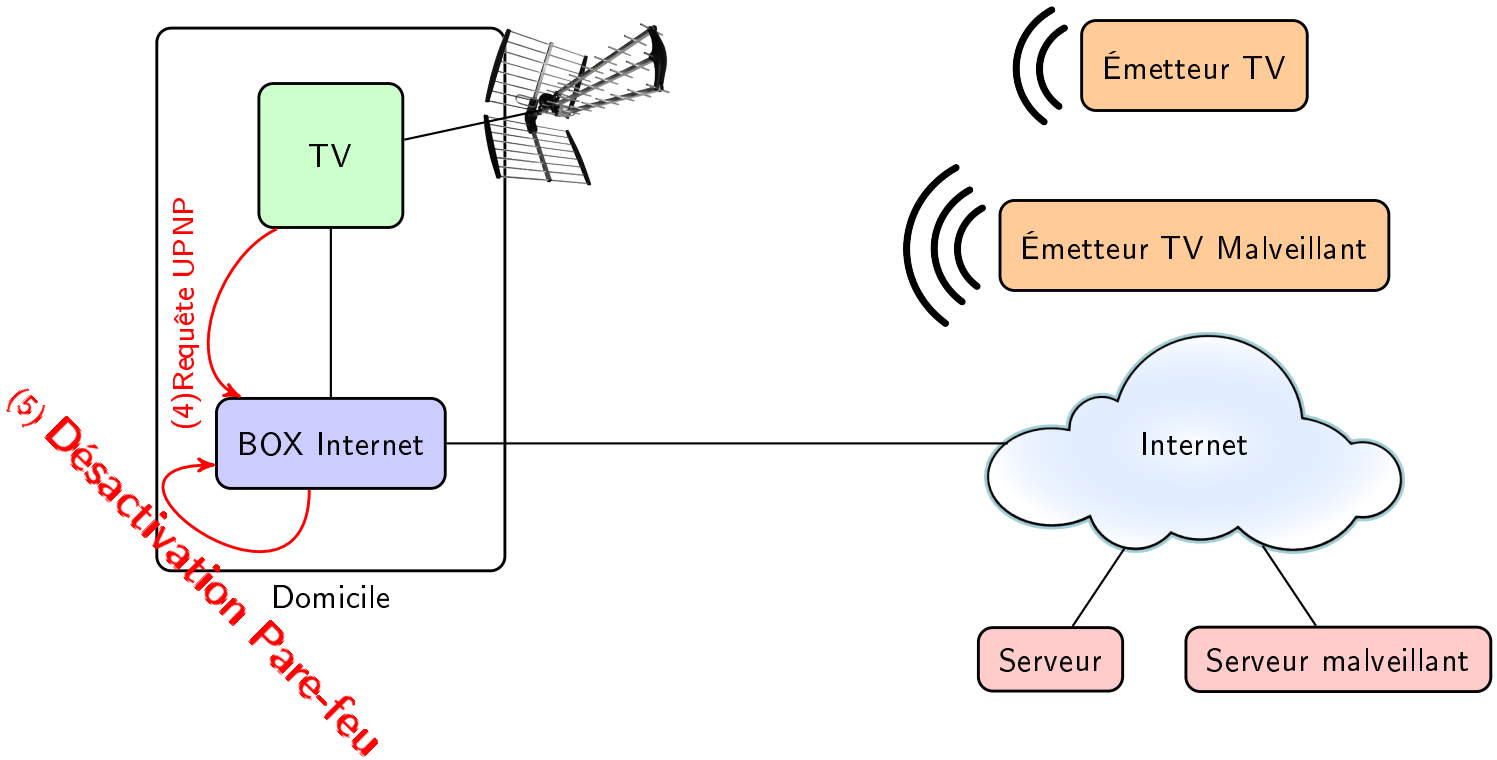
Application Malveillante



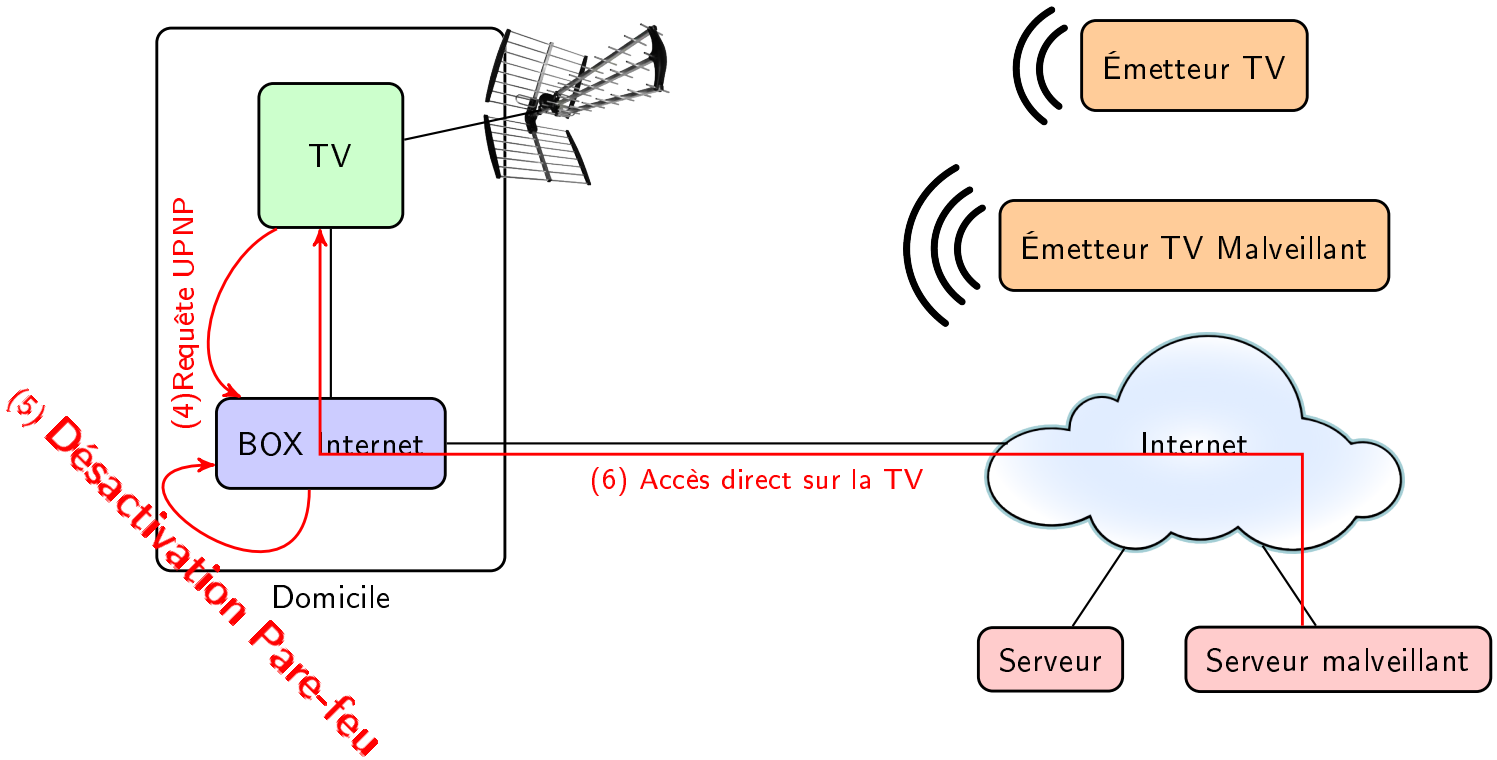
Application Malveillante



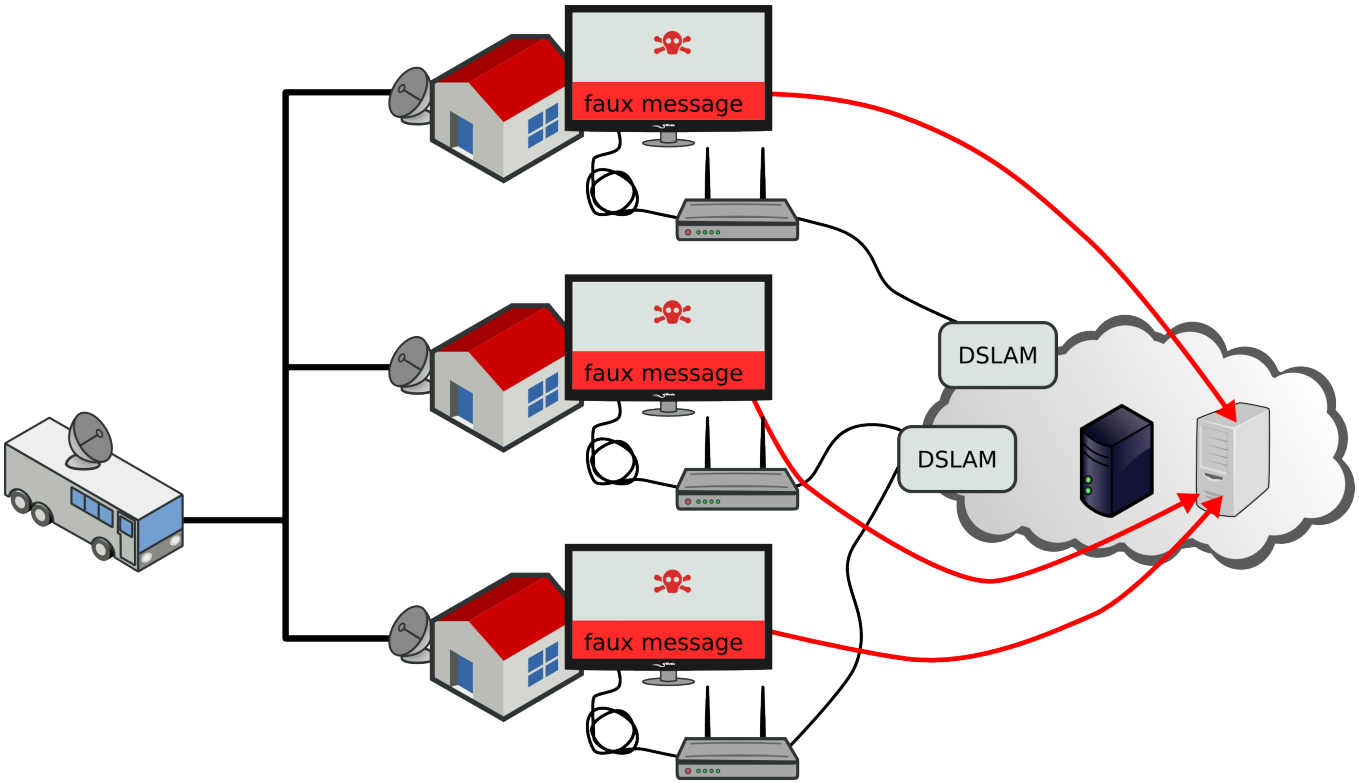
Application Malveillante



Application Malveillante



Généralisation de l'attaque



- Diffusion depuis un point fortement habité
- Prise de contrôle de plusieurs TV ⇒ Constitution d'un *botnet* de TV

Bilan

La recherche de vulnérabilités

- Est un aspect à ne pas négliger
- Est complémentaire des méthodes formelles
- Doit être mené au cours du développement et non sur le produit final

Perspectives

Importance des études de sécurité pour l'IoT

- Equipements de plus en plus intelligents
- Connectivité des équipements de plus en plus importante
- *Le risque peut se cacher derrière des équipements associés à un usage banal*

$\Rightarrow$ La prise en compte la sécurité de ces objets est fondamentale

$\Rightarrow$ Besoin de méthodes pour évaluer ces objets

$\Rightarrow$ Etudier en particulier les liens de communications, vecteur de propagation de maliciels, qui nécessitent des études ciblées étant donné le nombre et la diversité de ces liens.