Sécurité des équipements grand public connectés à Internet

évaluation des liens de communication

Yann Bachy

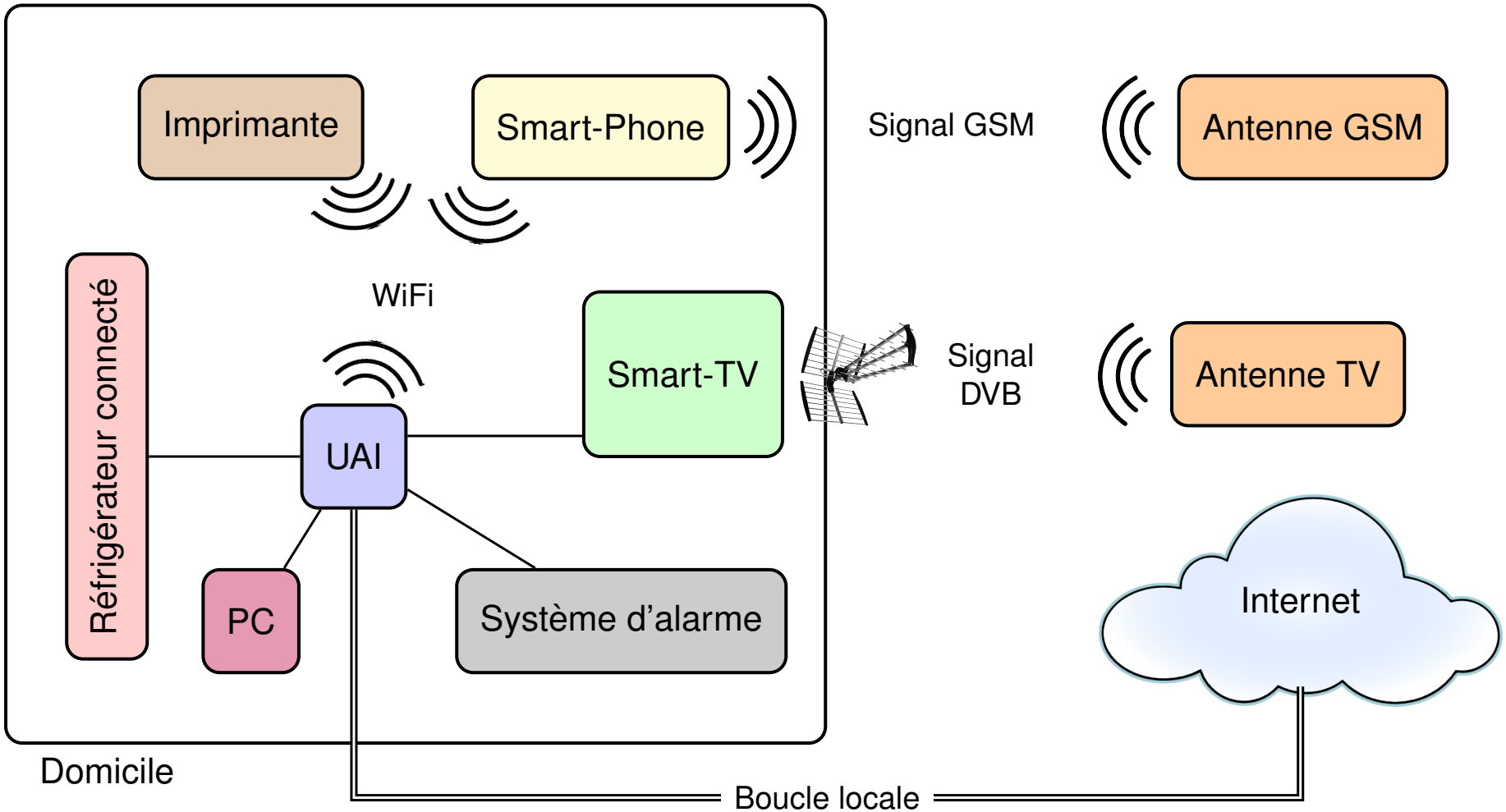
ISAE-SUPAERO département DISC
Travaux réalisés au LAAS-CNRS dans l'équipe TSF

12 avril 2016

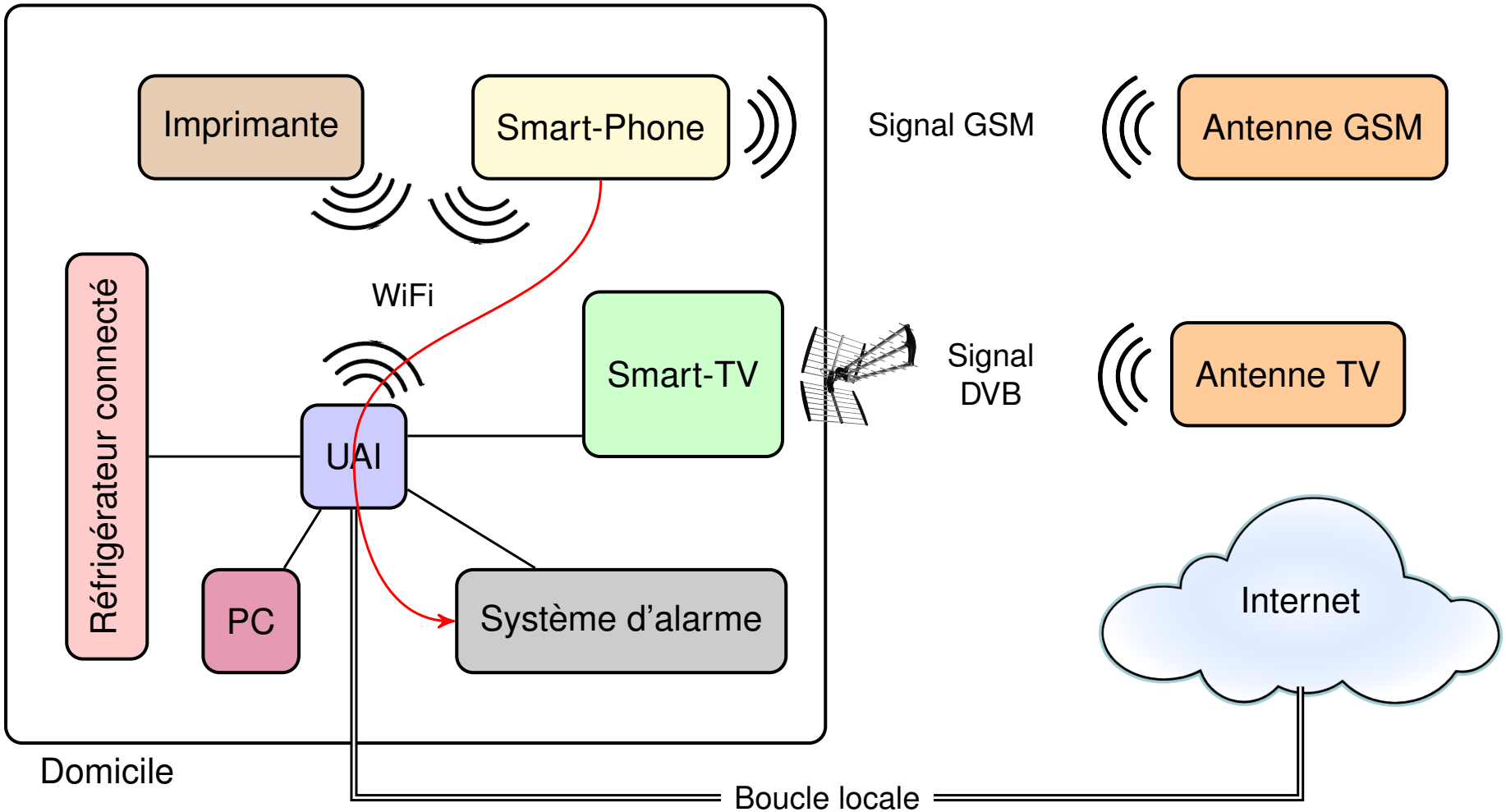
Émergence des équipements connectés à Internet

- Des équipements proposant de plus en plus de services
- Une interconnexion massive avec le réseau Internet

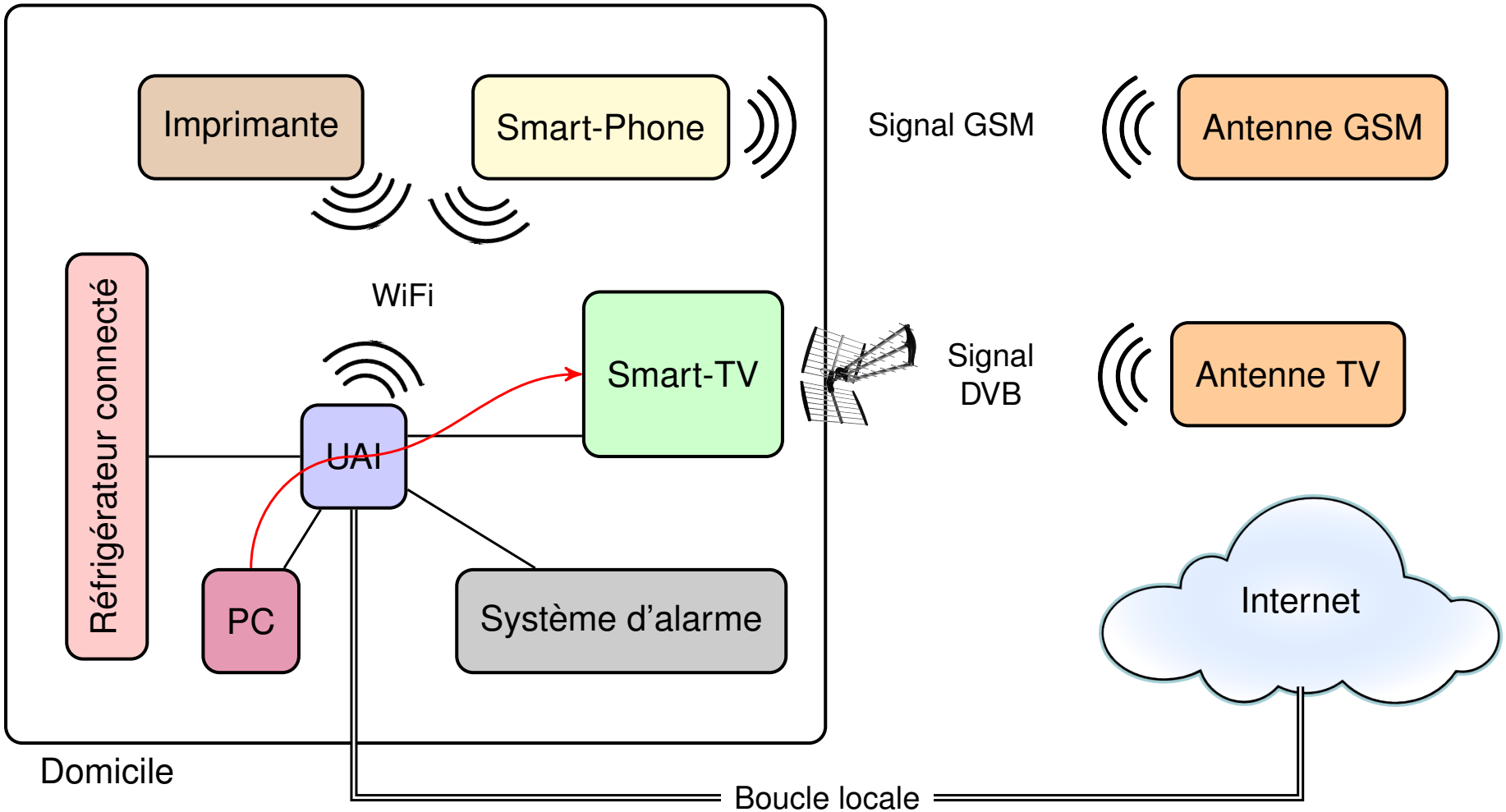
Le réseau Internet domestique



Le réseau Internet domestique



Le réseau Internet domestique



Problématique

- Équipements qui peuvent être compromis pour exécuter du code malveillant
- Risque de vulnérabilités accru dû à une maintenance tardive ou inexistante
- Pas de garantie du respect de la vie privée de l'utilisateur
- Surface d'attaque augmentée par le nombre d'interfaces de communications

L'équipement connecté à plusieurs réseaux peut être utilisé comme relai, une fois compromis, pour attaquer d'autres équipements du domicile

Objectifs

Guider les analyses de vulnérabilités d'équipements connectés

- Définir une méthode d'analyse
- Permettre une identification systématique des scénarios d'attaque et évaluer techniquement leur faisabilité
- Focus particulier sur les liens de communication

Application de la méthode

- Unités d'Accès Intégrées (UAI)
- Téléviseurs connectés (Smart-TV)

Plan

Méthode d'analyse

Identification des risques

- Utilisation des méthodes industrielles existantes permettant d'analyser les risques d'un système

Validation technique de ces risques

- Suite d'expérimentations dans le but de valider techniquement les risques identifiés

Étude des contre-mesures

- Étudier les contre-mesures existantes permettant de réduire ou annuler le risque étudié
- *ou* Proposer de nouvelles méthodes

Méthode d'analyse

Identification des risques

- Utilisation des méthodes industrielles existantes permettant d'analyser les risques d'un système

Validation technique de ces risques

- Suite d'expérimentations dans le but de valider techniquement les risques identifiés

Étude des contre-mesures

- Étudier les contre-mesures existantes permettant de réduire ou annuler le risque étudié
- *ou* Proposer de nouvelles méthodes

Les méthodes d'analyse des risques

Comparaison des méthodes

- MEHARI (France, CLUSIF)
- EBIOS (France, ANSSI)
- CRAMM (Royaume Uni)
- OCTAVE (USA)

Les méthodes d'analyse des risques

Comparaison des méthodes

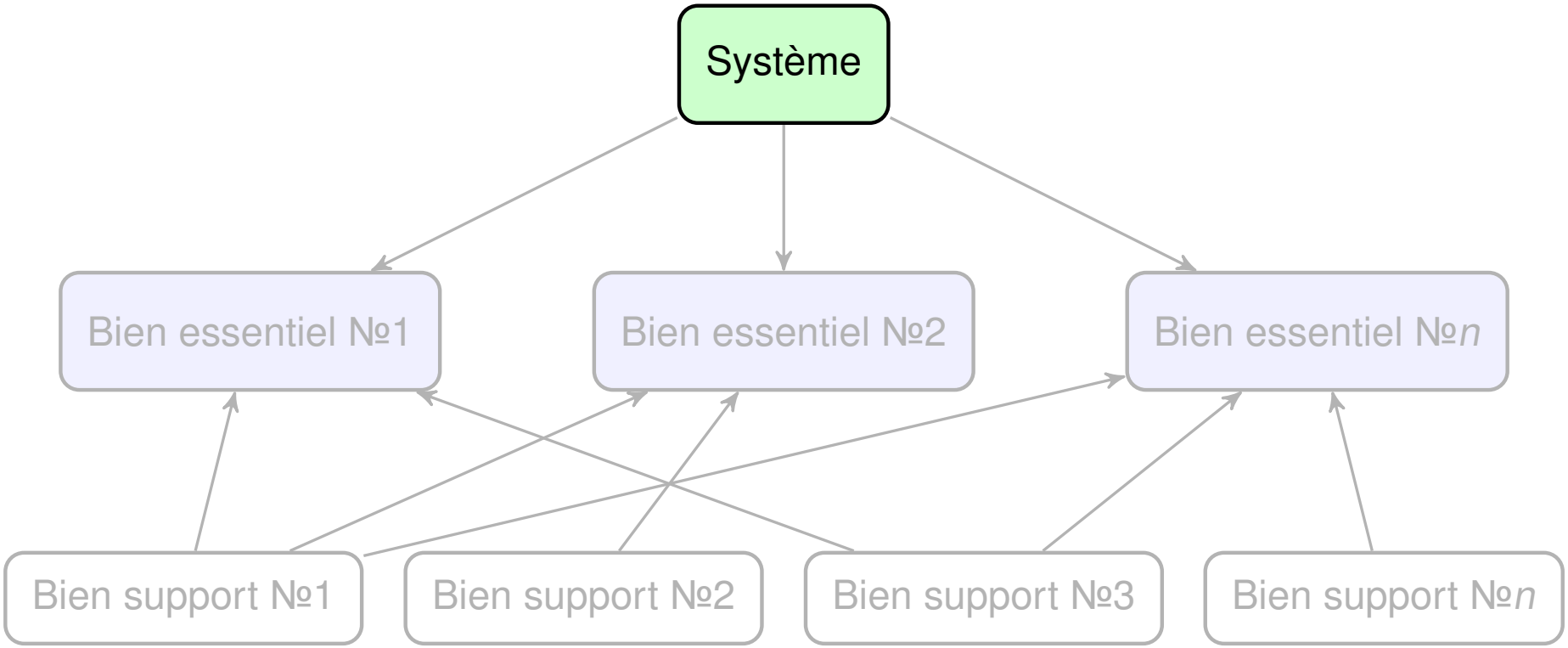
- MEHARI (France, CLUSIF)
- EBIOS (France, ANSSI)
- CRAMM (Royaume Uni)
- OCTAVE (USA)

EBIOS

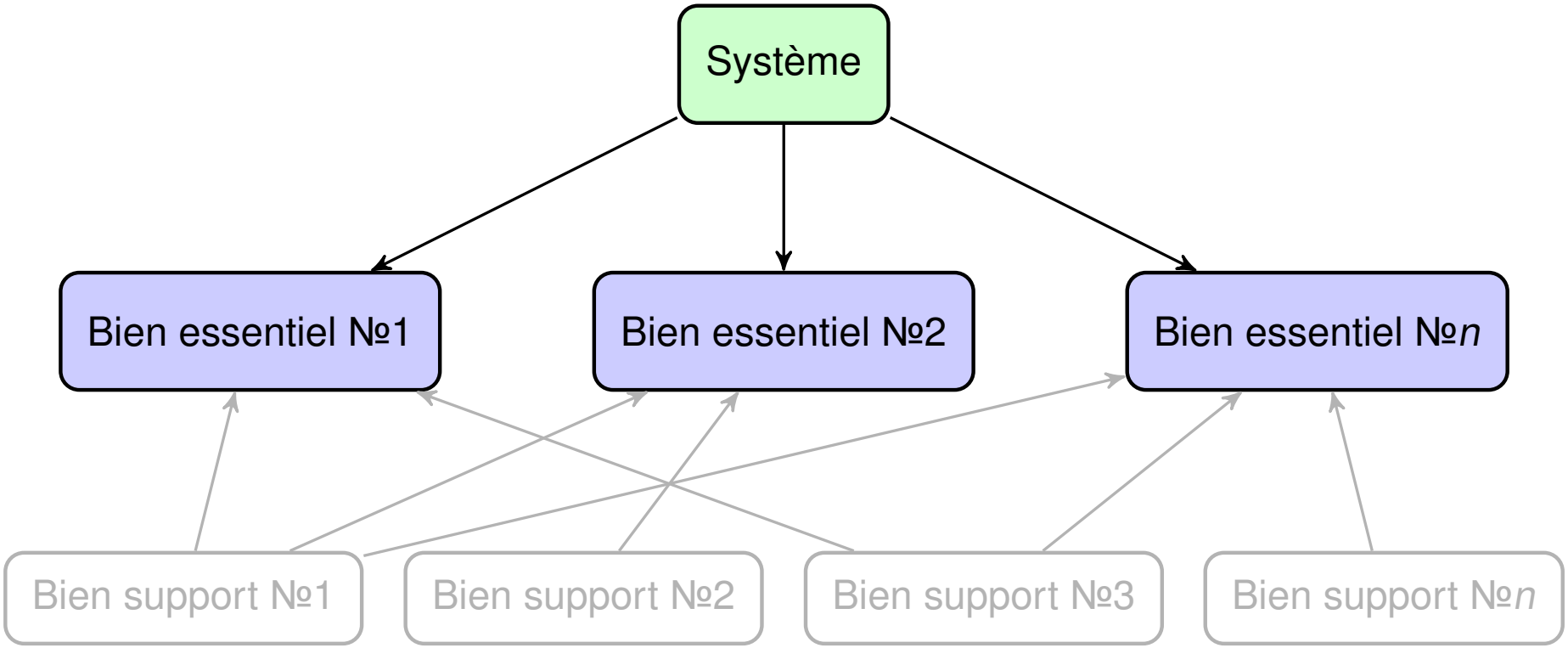
Expression des Besoins et Identification des Objectifs de Sécurité

- Massivement utilisée en France
- Une méthode générique, adaptable à n'importe quel contexte
- Inclut une base de connaissances issues de l'expérience

La méthode EBIOS

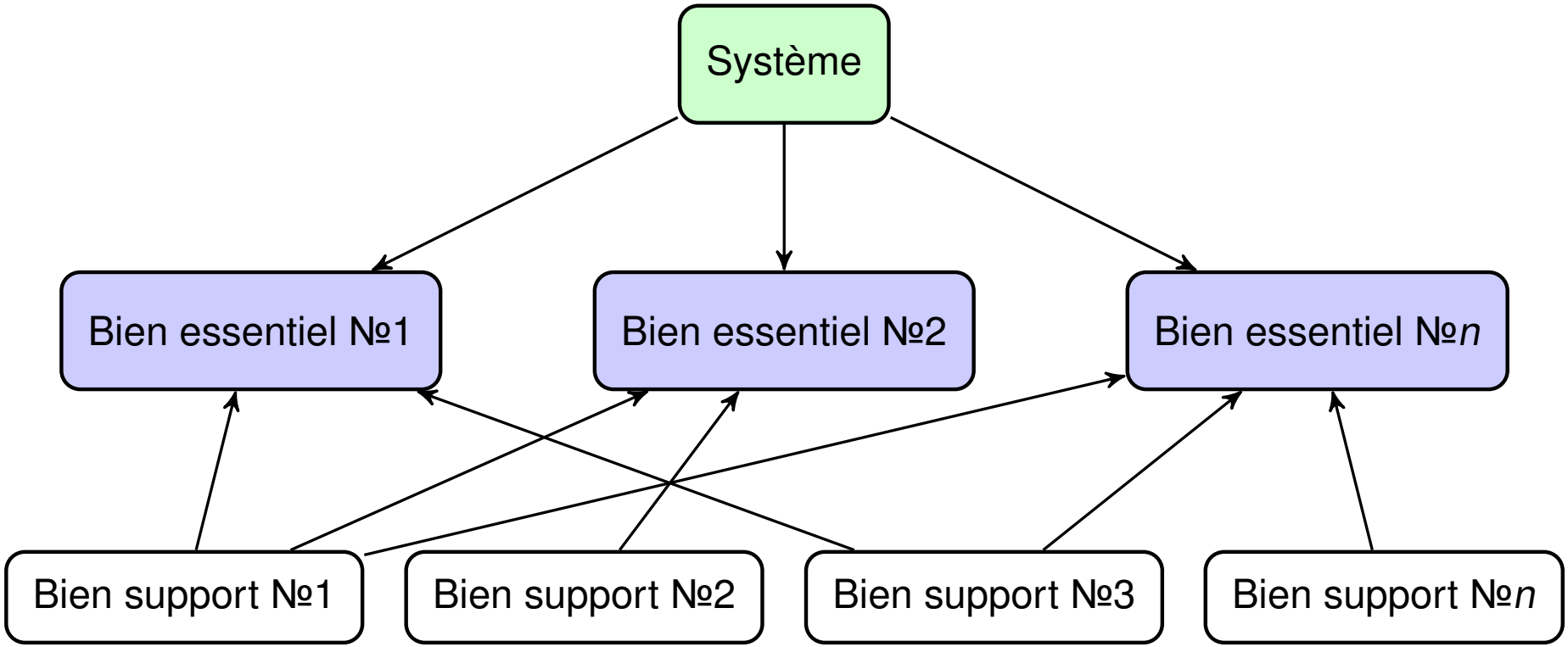


La méthode EBIOS



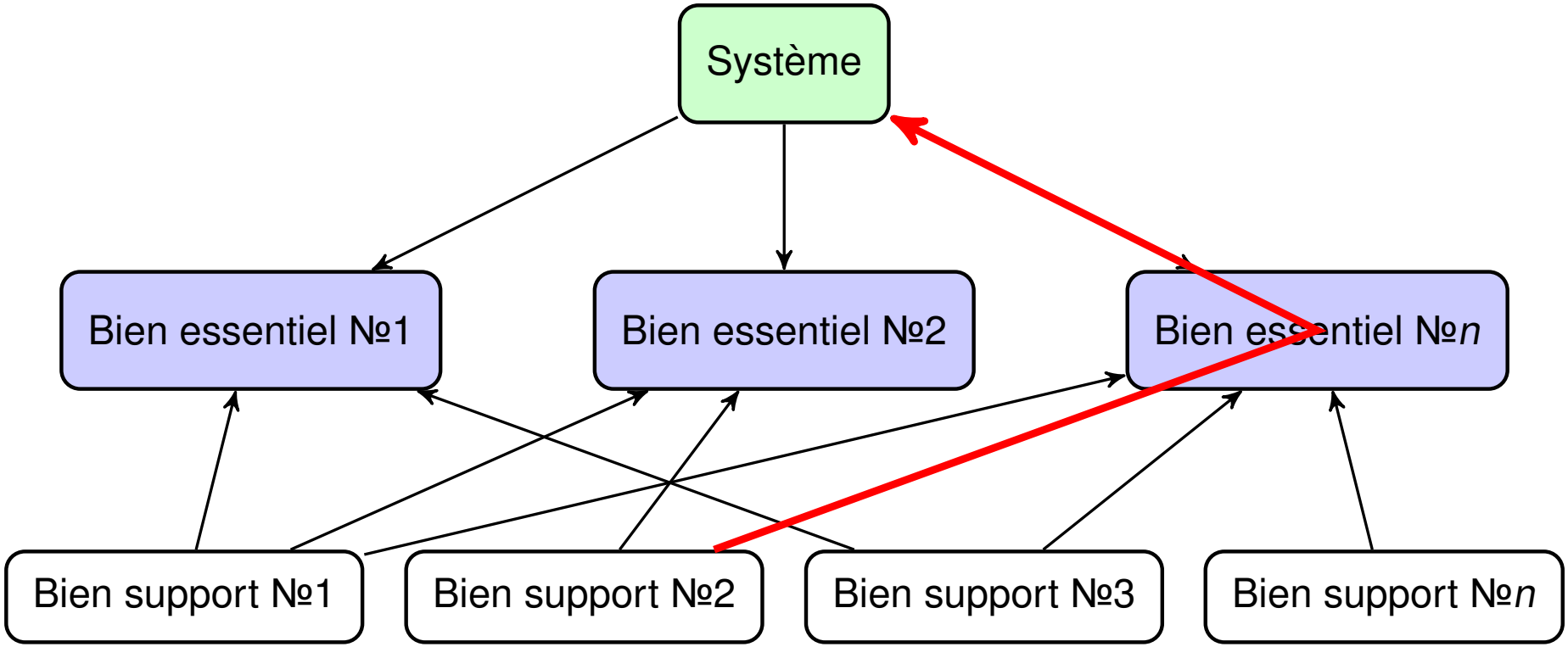
Les fonctions primaires, non tangibles, réalisées par le système. Leur compromission est évaluée selon leur gravité.

La méthode EBIOS



Les biens supports, tangibles, permettant la réalisation des fonctions primaires.
Leur compromission est évaluée selon leur vraisemblance.

La méthode EBIOS



risque

=

vraisemblance de la compromission d'un bien support

x

la gravité de la compromission d'un bien essentiel

Classification des risques

	Vraisemblance		
Gravité	Minime	Significative	Maximale
Négligeable			
Limitée			
Importante			
Critique			

Méthode d'analyse

Identification des risques

- Utilisation des méthodes industrielles existantes permettant d'analyser les risques d'un système

Validation technique de ces risques

- Suite d'expérimentations dans le but de valider techniquement les risques identifiés

Étude des contre-mesures

- Étudier les contre-mesures existantes permettant de réduire ou annuler le risque étudié
- *ou* Proposer de nouvelles méthodes

Validation technique des risques identifiés

Observation passive

- Observer toute communication sur le lien de communication visé
- Comprendre le fonctionnement des protocoles mis en œuvre

Validation technique des risques identifiés

Observation passive

- Observer toute communication sur le lien de communication visé
- Comprendre le fonctionnement des protocoles mis en œuvre

Simulation

- Simuler l'environnement de l'équipement étudié
- Se substituer aux fournisseurs de services légitimes

Validation technique des risques identifiés

Observation passive

- Observer toute communication sur le lien de communication visé
- Comprendre le fonctionnement des protocoles mis en œuvre

Simulation

- Simuler l'environnement de l'équipement étudié
- Se substituer aux fournisseurs de services légitimes

Conduite d'attaques

- Injection d'attaques dans l'environnement simulé

Méthode d'analyse

Identification des risques

- Utilisation des méthodes industrielles existantes permettant d'analyser les risques d'un système

Validation technique de ces risques

- Suite d'expérimentations dans le but de valider techniquement les risques identifiés

Étude des contre-mesures

- Étudier les contre-mesures existantes permettant de réduire ou annuler le risque étudié
- *ou* Proposer de nouvelles méthodes

Étude des contre-mesures

Identification des besoins

- Évaluer le besoin selon chaque critère de sécurité (Disponibilité, Intégrité, Confidentialité et Authenticité)

Étude des contre-mesures

Identification des besoins

- Évaluer le besoin selon chaque critère de sécurité (Disponibilité, Intégrité, Confidentialité et Authenticité)

Identification des mesures de sécurité existantes

- Étude des normes et références liées au sous-système étudié
- Dans le cadre des liens de communication, étude de chaque niveau de la pile de protocoles employée

Étude des contre-mesures

Identification des besoins

- Évaluer le besoin selon chaque critère de sécurité (Disponibilité, Intégrité, Confidentialité et Authenticité)

Identification des mesures de sécurité existantes

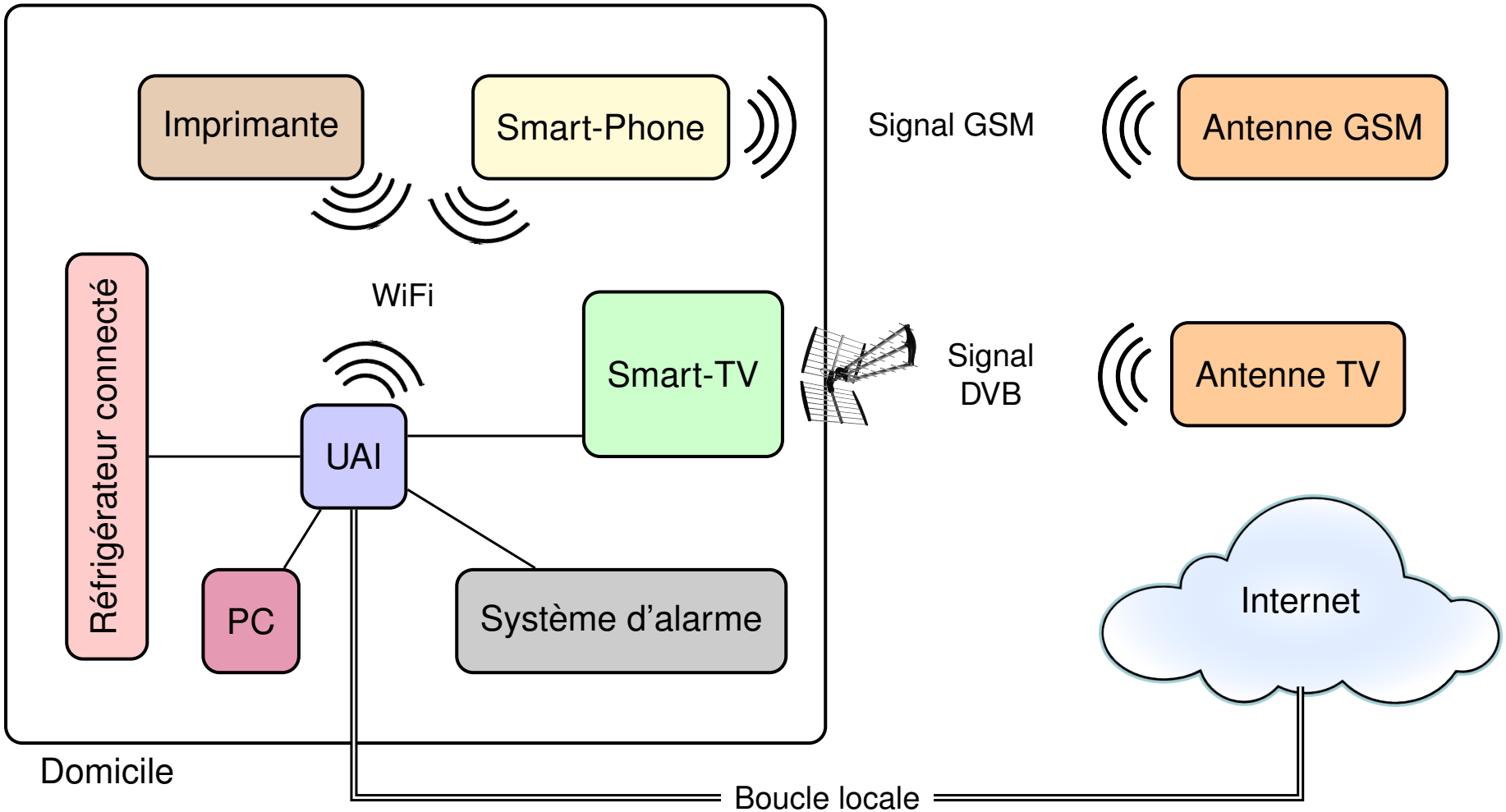
- Étude des normes et références liées au sous-système étudié
- Dans le cadre des liens de communication, étude de chaque niveau de la pile de protocoles employée

Proposition de contre-mesures

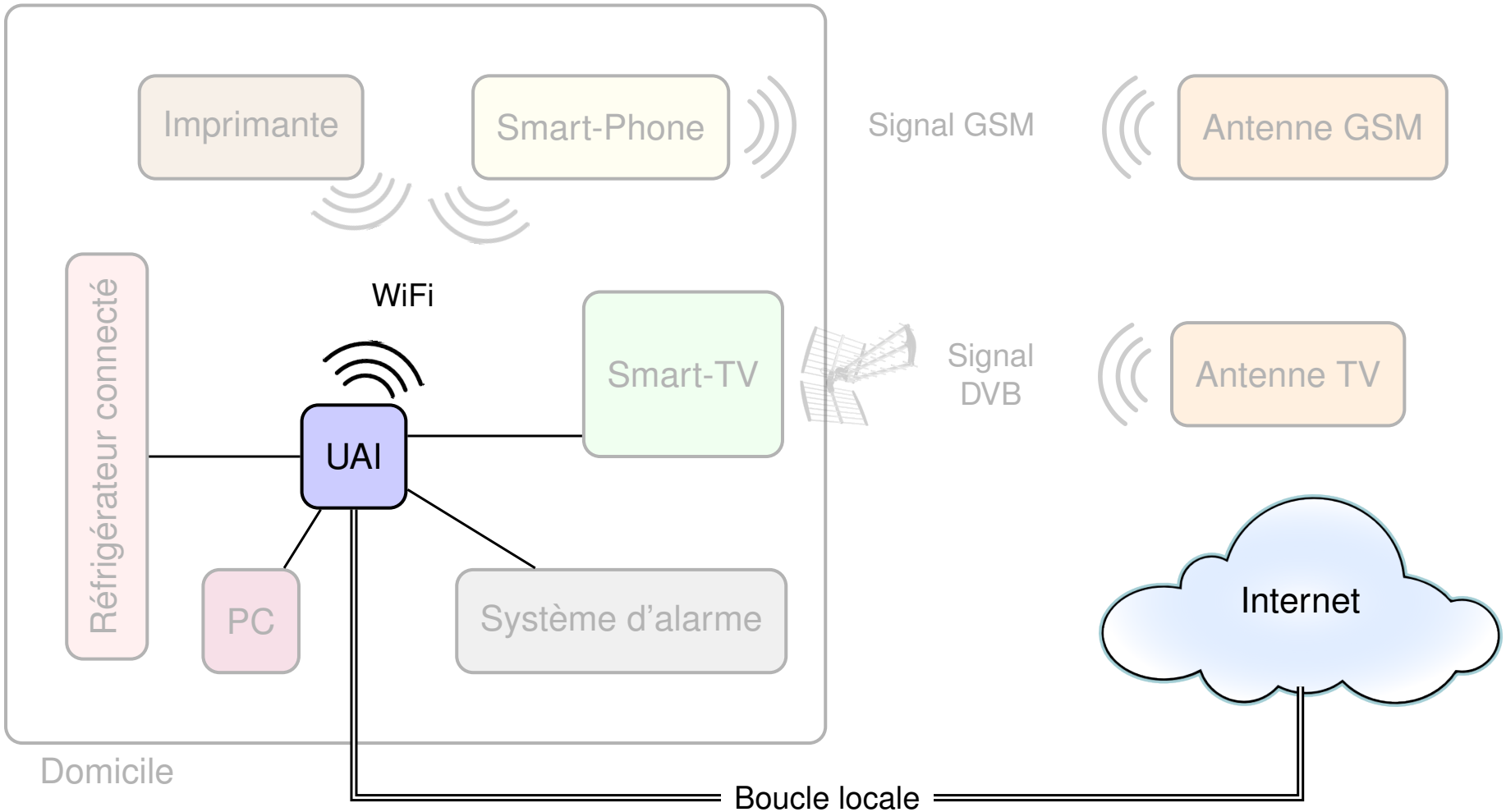
- En cas d'absence de mécanismes de sécurité pertinents face au risque étudié, proposer de nouveaux mécanismes

Plan

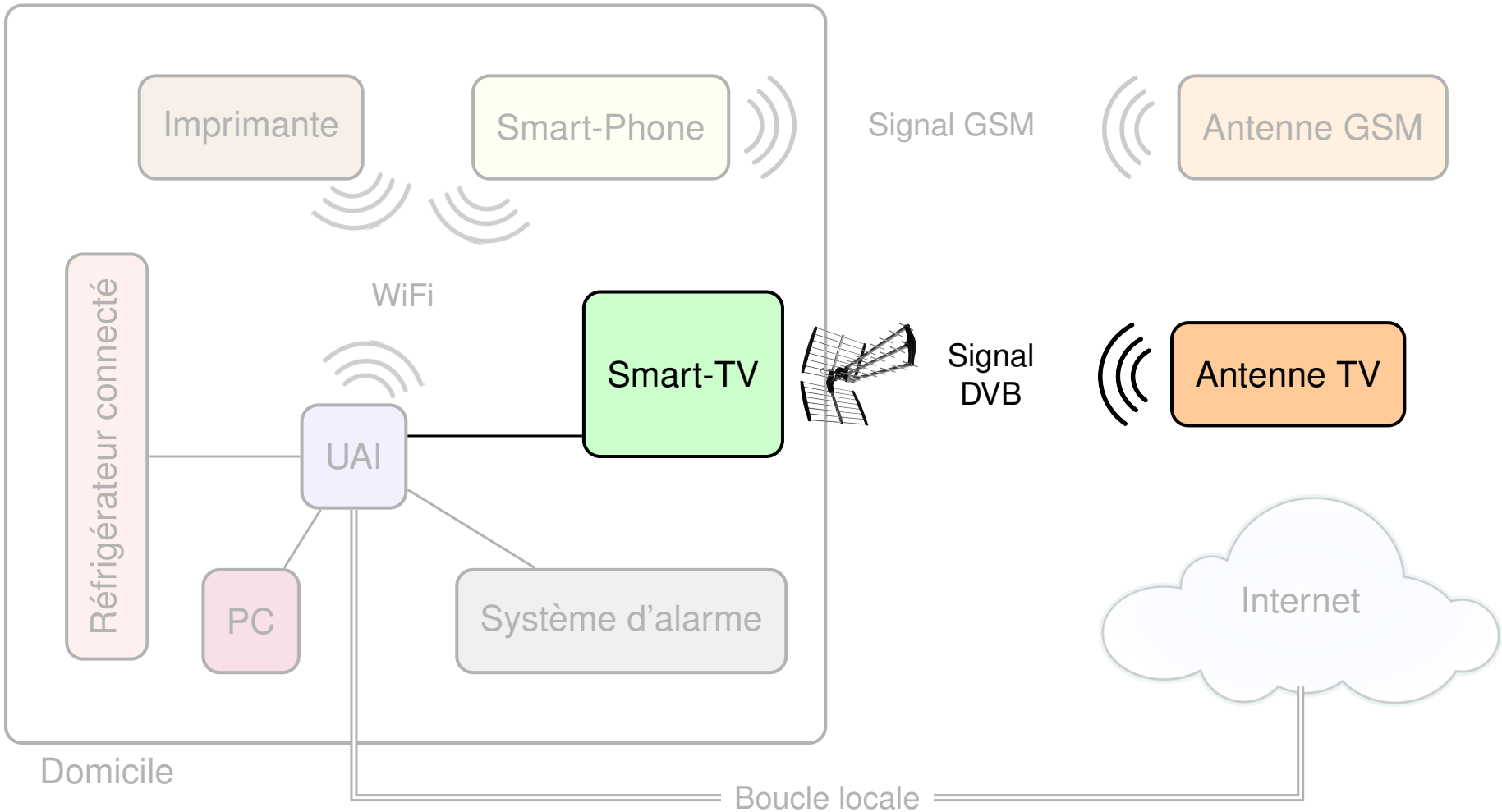
Études de cas



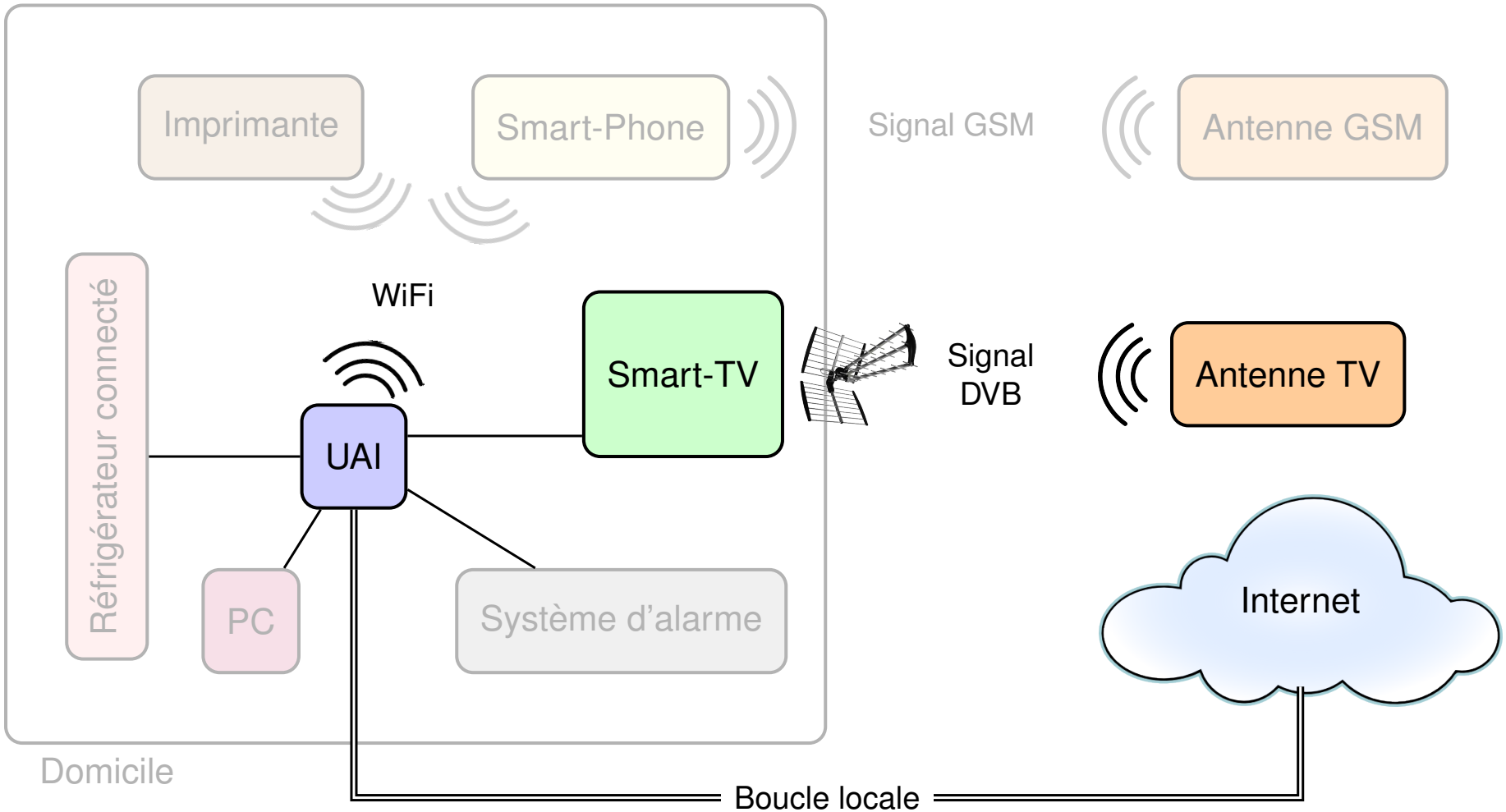
Études de cas



Études de cas



Études de cas



Risques identifiés pour l'UAI

	Vraisemblance		
Gravité	Minime	Significative	Maximale
Négligeable	TV non confidentiel	NAS non accessible NAS non confidentiel Web non intègre	NAS non authentique TV non authentique
Limitée		TV non disponible TV non intègre	
Importante	TEL non confidentiel	TEL non intègre Web non disponible	Web non authentique
Critique		TEL non disponible NAS non intègre Web non confidentiel	

Risques identifiés pour l'UAI

	Vraisemblance		
Gravité	Minime	Significative	Maximale
Négligeable	TV non confidentiel	NAS non accessible NAS non confidentiel Web non intègre	NAS non authentique TV non authentique
Limitée		TV non disponible TV non intègre	
Importante	TEL non confidentiel	TEL non intègre Web non disponible	Web non authentique
Critique		TEL non disponible NAS non intègre Web non confidentiel	

Risques identifiés pour les Smart-TV

	Vraisemblance		
Gravité	Minime	Significative	Maximale
Négligeable	PVR non disponible LMR non disponible	TV interactive non disponible	
Limité	VoD non intègre LMR non intègre	VoD non disponible VoD non authentique PVR non authentique	TV non intègre PVR non intègre TV interactive non intègre
Importante		TV non confidentiel TV non authentique VoD non confidentiel PVR non confidentiel TV interactive non confidentiel LMR non confidentiel LMR non authentique	
Critique	TV non disponible	TV interactive non authentique	

Risques identifiés pour les Smart-TV

	Vraisemblance		
Gravité	Minime	Significative	Maximale
Négligeable	PVR non disponible LMR non disponible	TV interactive non disponible	
Limité	VoD non intègre LMR non intègre	VoD non disponible VoD non authentique PVR non authentique	TV non intègre PVR non intègre TV interactive non intègre
Importante		TV non confidentiel TV non authentique VoD non confidentiel PVR non confidentiel TV interactive non confidentiel LMR non confidentiel LMR non authentique	
Critique	TV non disponible	TV interactive non authentique	

Les liens de communication concernés

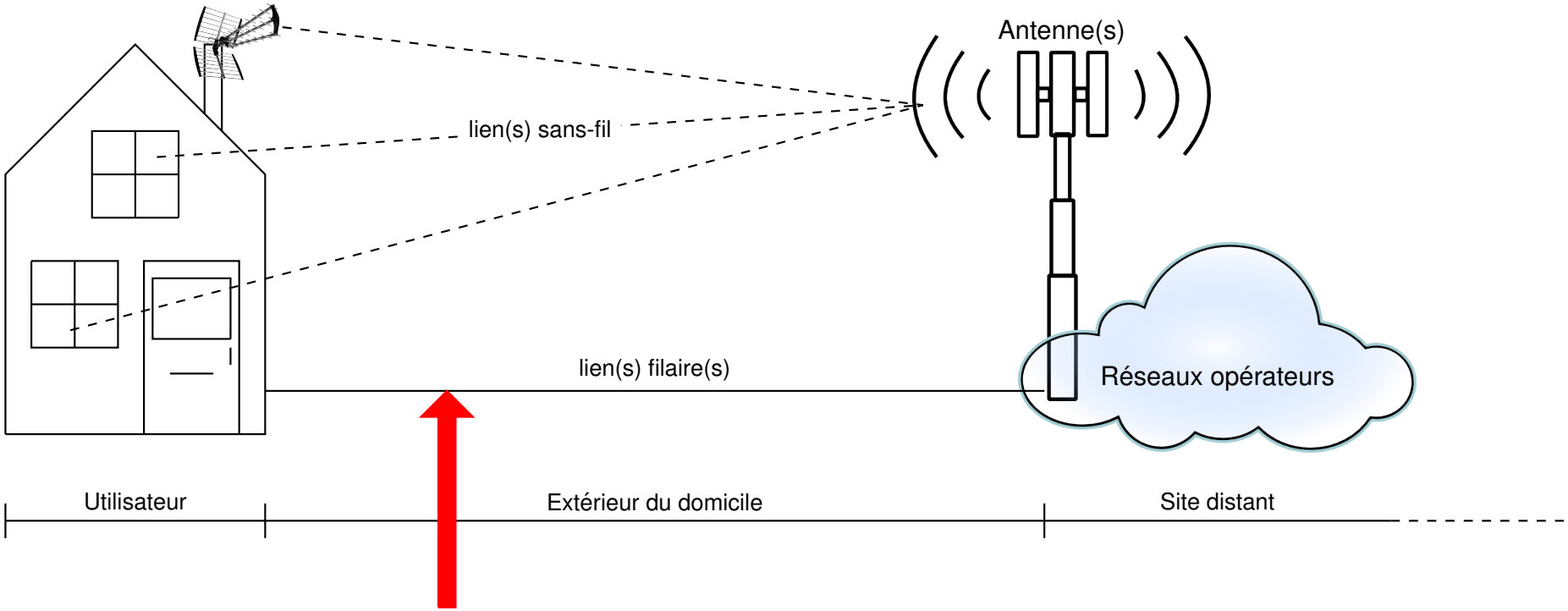
La boucle locale

- Lien privilégié entre le domicile et les services Internet
- Peu étudié dans la littérature

Le flux TV aérien

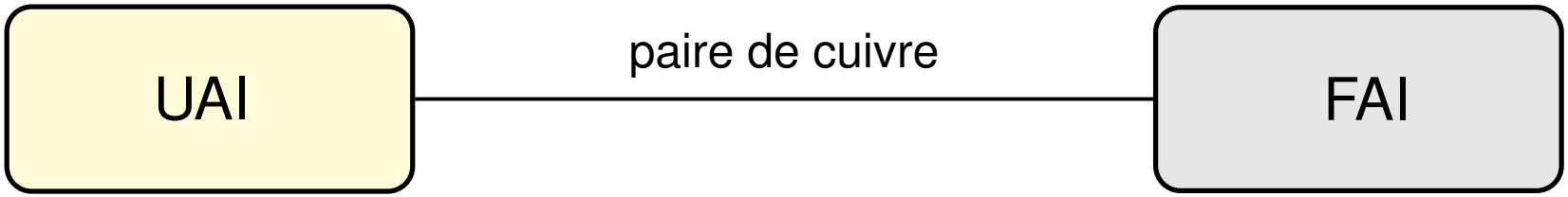
- Lien uni-directionnel, pas considéré comme cible d'attaque
- Des travaux théoriques, sans preuve expérimentale

La boucle locale

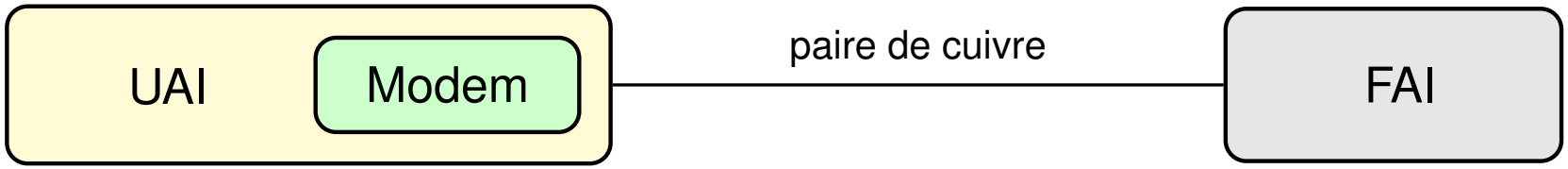


1. Observer toute communication sur ce lien
2. Simuler le fournisseur du service visé
3. Injecter des attaques

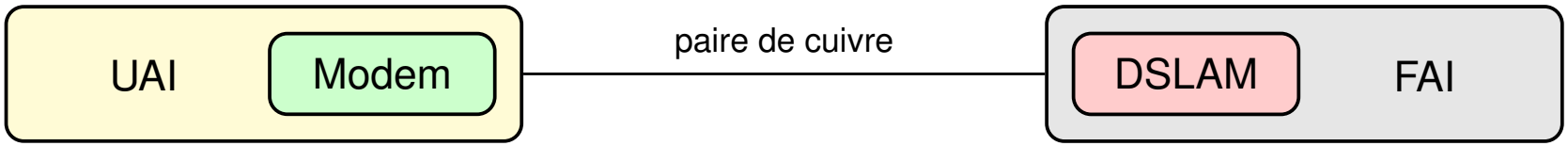
Écoute d'une boucle locale Internet



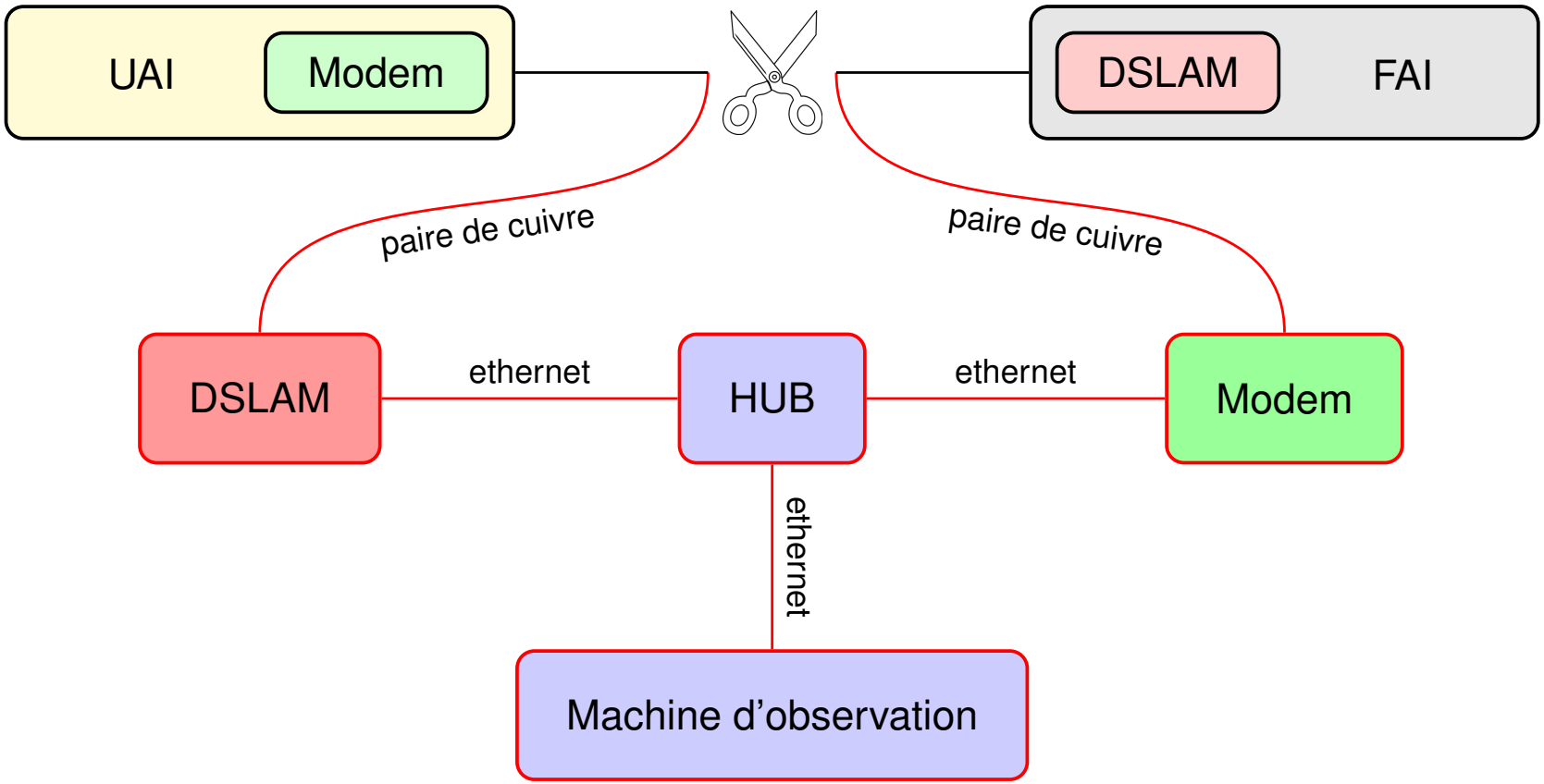
Écoute d'une boucle locale Internet



Écoute d'une boucle locale Internet



Écoute d'une boucle locale Internet



Expériences

Phase de démarrage et de mise à jour des UAI

- La phase de configuration contient potentiellement des informations sensibles
- Le firmware est un élément très sensible d'un point de vue sécurité pour les UAI

Lien Internet des téléviseurs connectés

- Mise à jour du firmware des téléviseurs par le lien Internet
- Seul lien sortant du domicile, les potentielles fuites de données privées peuvent uniquement passer sur ce lien

Comparaison de plusieurs UAI ADSL

Étude comparative de la phase de configuration et de mise à jour de six UAI ADSL déployées en France

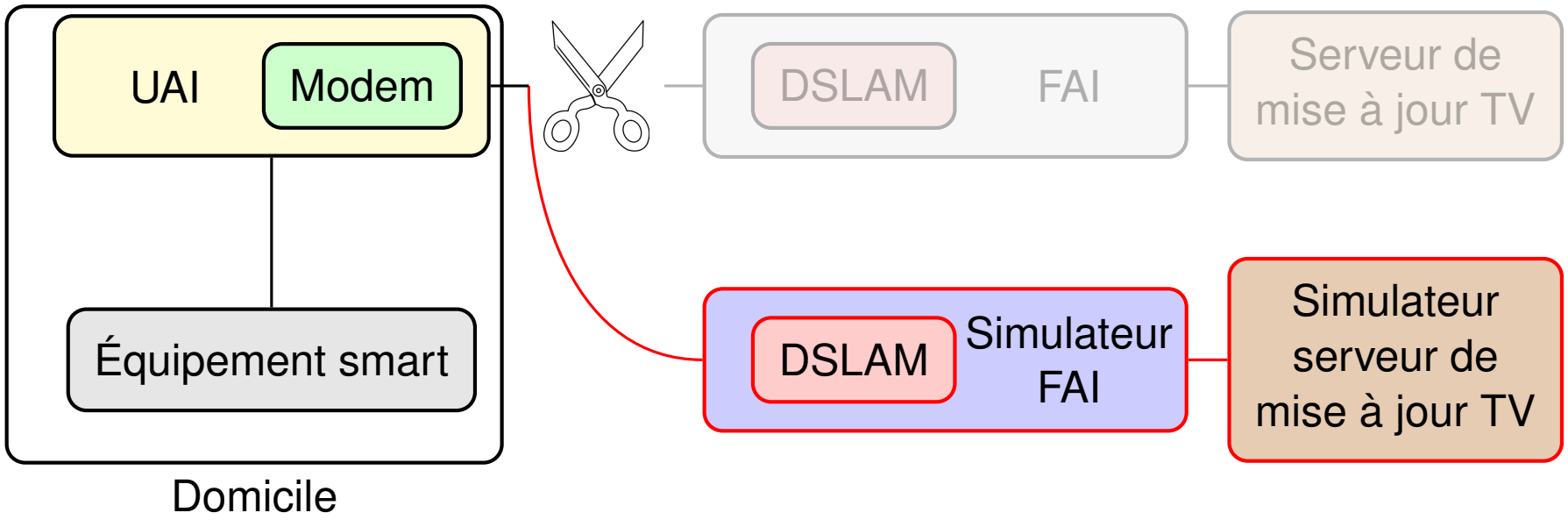
UAI	*A*	*B*	*C*	*D*	*E*	*F*
Configuration	HTTP + FTP + HTTPS	HTTP + HTTPS	HTTPS	HTTP	HTTP	HTTPS
Mise à jour	?	HTTPS	?	HTTP	HTTP	?

Procédures de mise à jour des Smart-TV

Étude comparative de la phase de mise à jour de quatre Smart-TV

TV		*A*	*B*	*C*	*D*
Négociation	protocol	HTTP	HTTP + HTTPS	HTTPS	HTTP
	content	unknown	XML + ?	?	XML
Transfert	protocol	HTTP	?	HTTP	HTTP
	content	Binary	?	Binary	Binary

Simulation de fournisseur de services Internet



Simulation du serveur de mise à jour des UAI ADSL et Smart-TV

Simulation du service de mise à jour (1/4)

1er démarrage

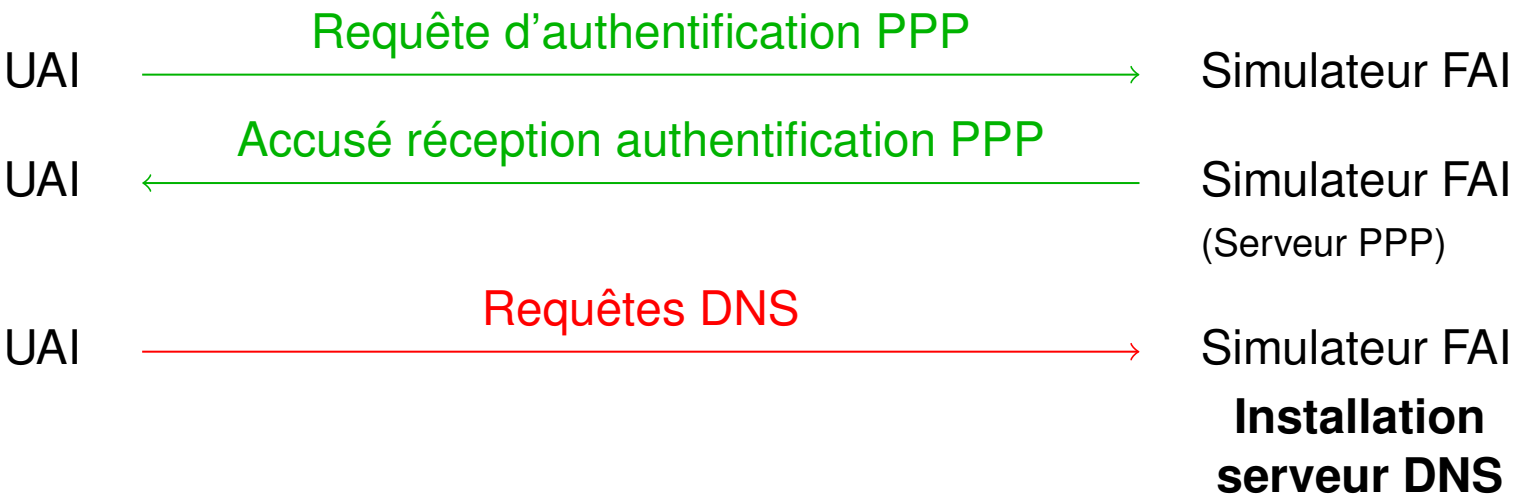
UAI —— Requête d'authentification PPP ——→ Simulateur FAI

Installation serveur PPP

redémarrage

Simulation du service de mise à jour (2/4)

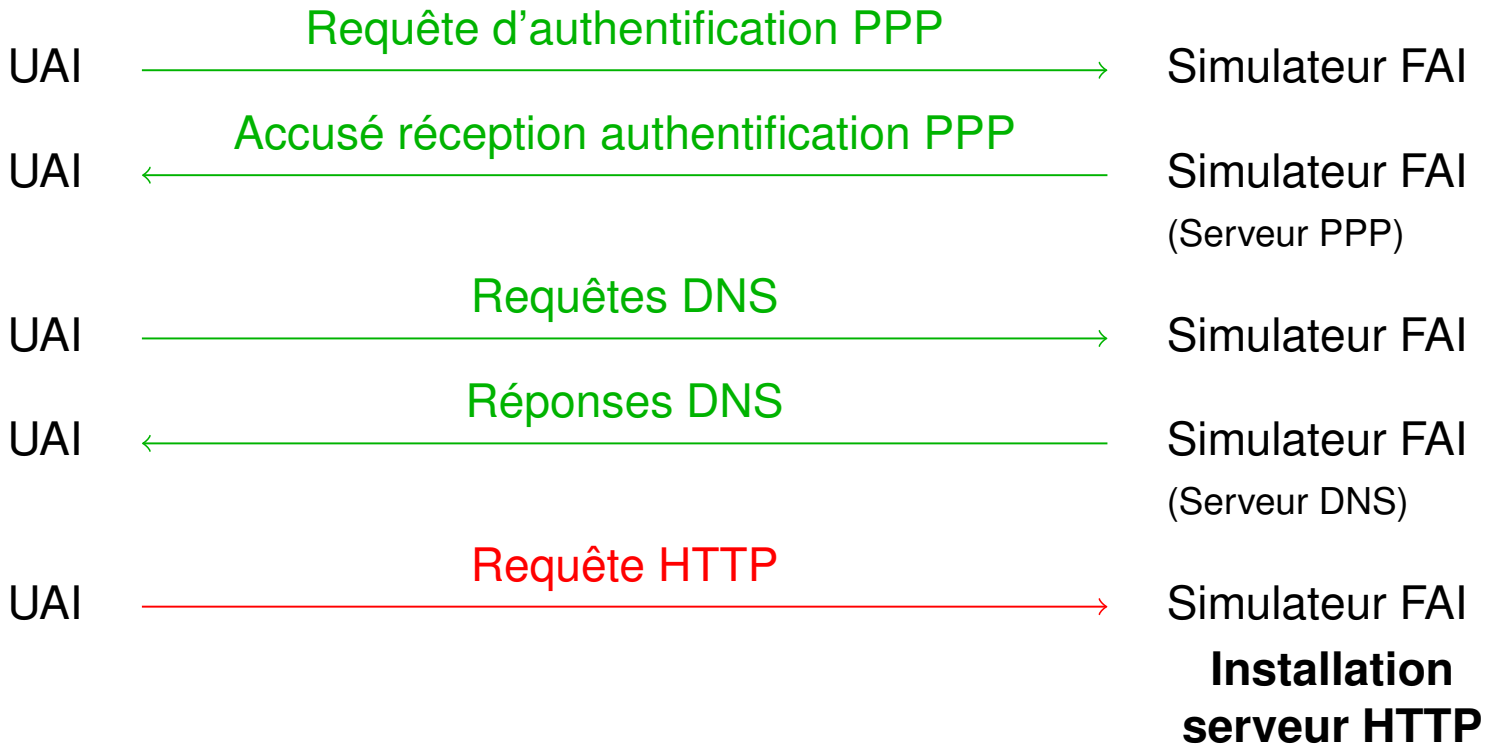
2nd démarrage



redémarrage

Simulation du service de mise à jour (3/4)

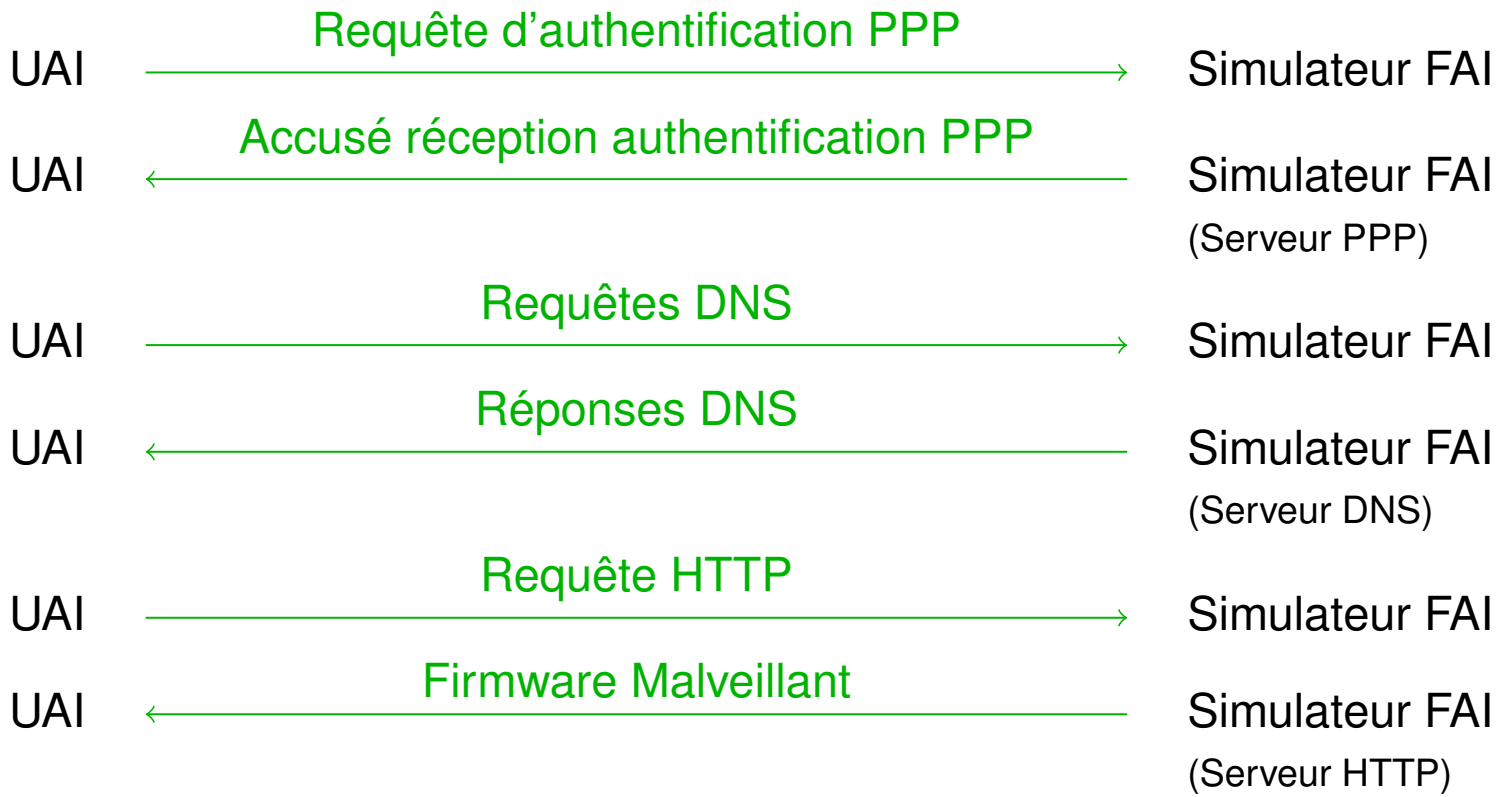
3ème démarrage



redémarrage

Simulation du service de mise à jour (4/4)

4ème démarrage



Résultats

Mise à jour UAI ADSL

- Mise à jour avec succès lorsque le protocole HTTP est utilisé
- Modifications dans le firmware :
  - Désactivation du pare-feu
  - Désactivation du service de mise à jour automatique
  - Installation d'un client SIP afin d'émettre des appels surtaxés

Mise à jour Smart-TV

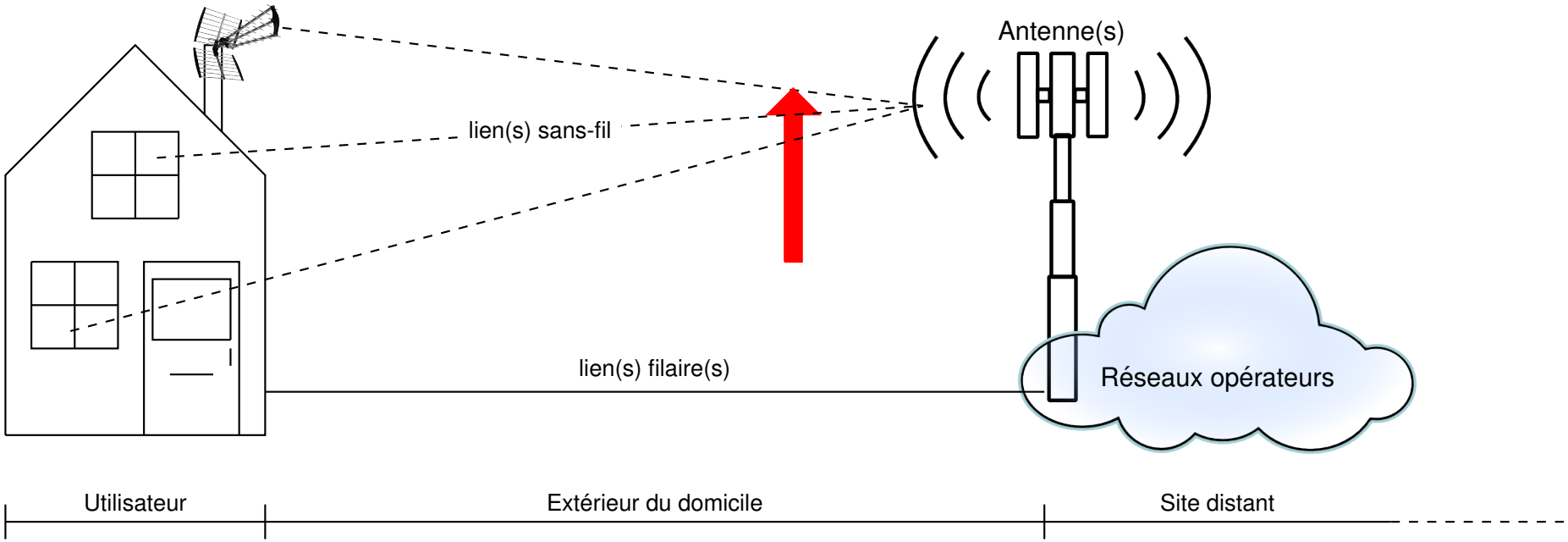
- Mise à jour anti-datée avec succès, uniquement sur le téléviseur *D*

→ Permet de ré-activer des vulnérabilités corrigées

- Procédures globalement bien sécurisées

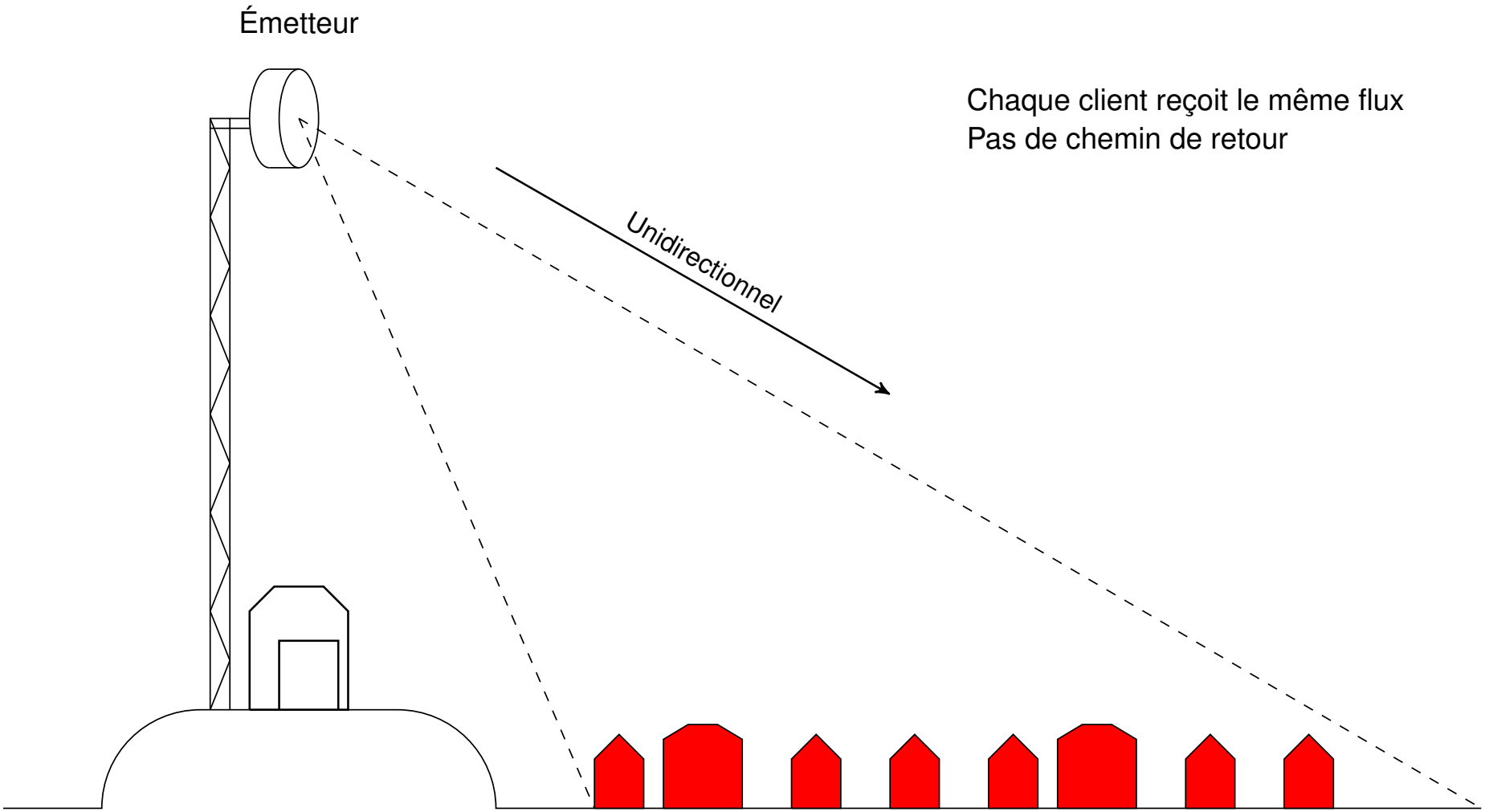
→ Grâce à l'utilisation d'une signature

Le flux TV aérien



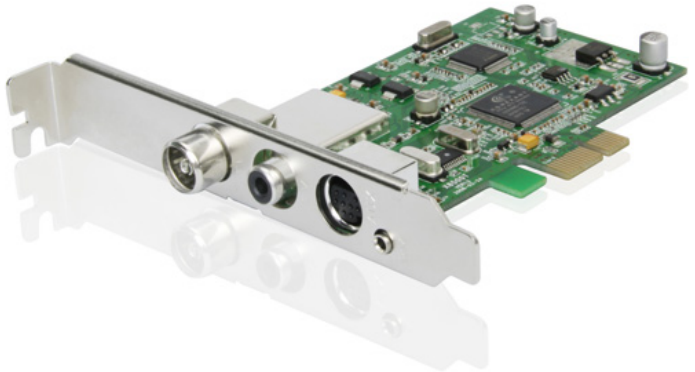
1. Observer toute communication sur ce lien
2. Simuler un émetteur TV
3. Injecter des attaques

Émission DVB



Chaque client reçoit le même flux
Pas de chemin de retour

Réception d'un signal DVB-T

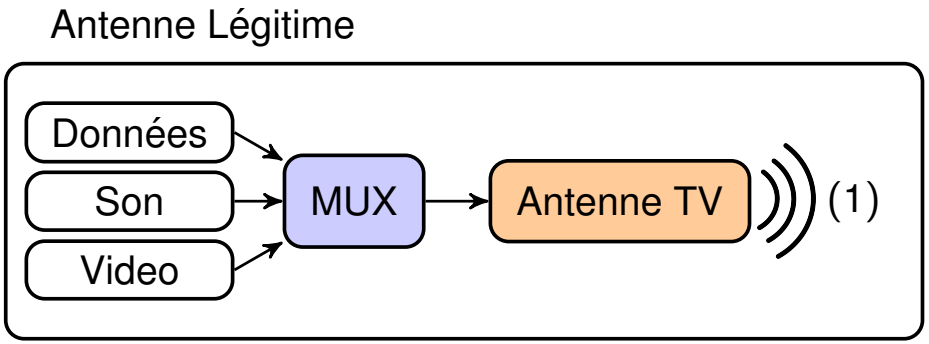


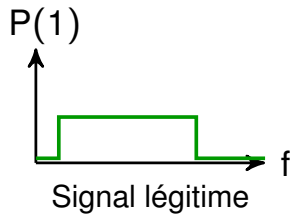
- Écoute = Réception
- Utilisation d'un démodulateur grand public
- Logiciel d'analyse de flux DVB open-source DVBSnoop

Émission d'un signal DVB-T

- Modulation haute fréquence
- Pas d'équipement grand public disponible
- Radio logicielle (*Software Defined Radio (SDR)*)
- Modulateur expérimental

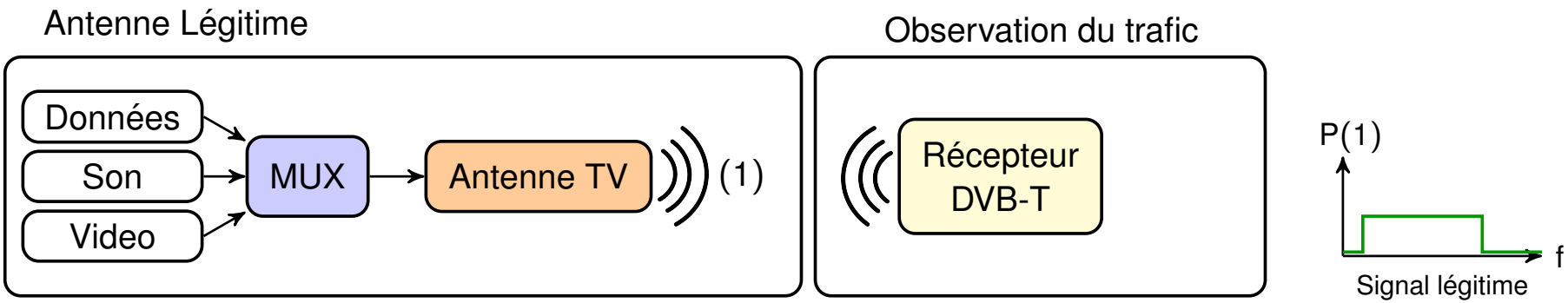
Plateforme d'expérimentations DVB-T





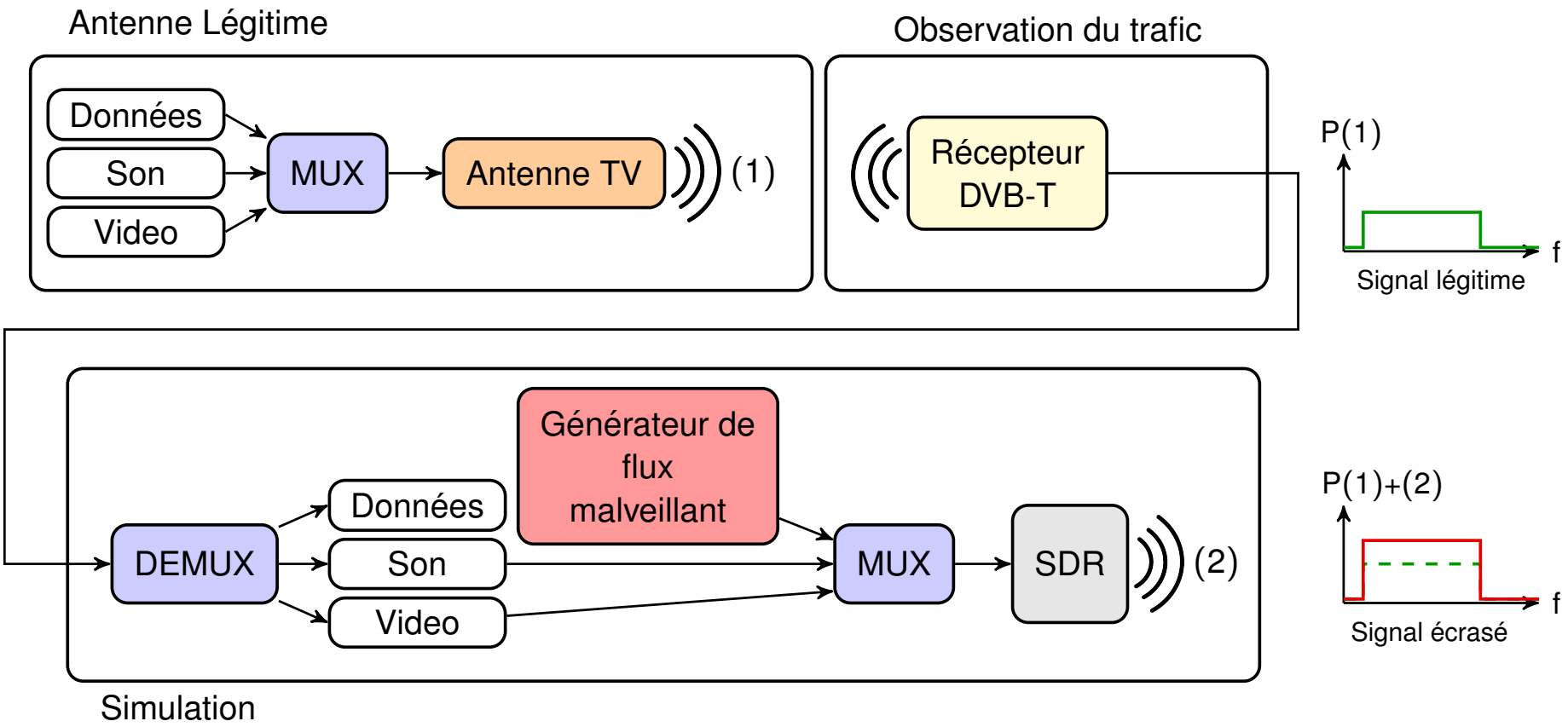
(1) = Signal légitime

Plateforme d'expérimentations DVB-T



(1) = Signal légitime

Plateforme d'expérimentations DVB-T

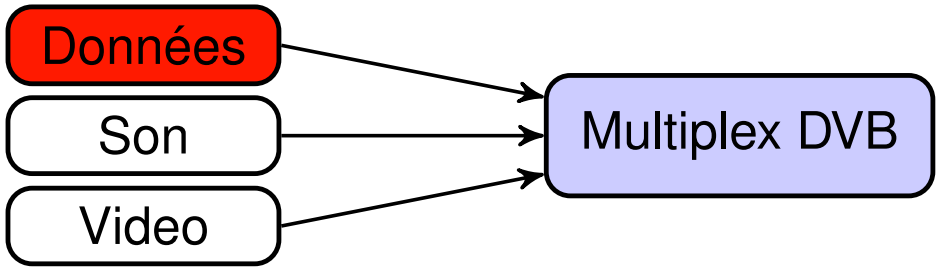


(1) = Signal légitime

(2) = Signal malveillant

Demo : modification du contenu Vidéo d'un flux DVB

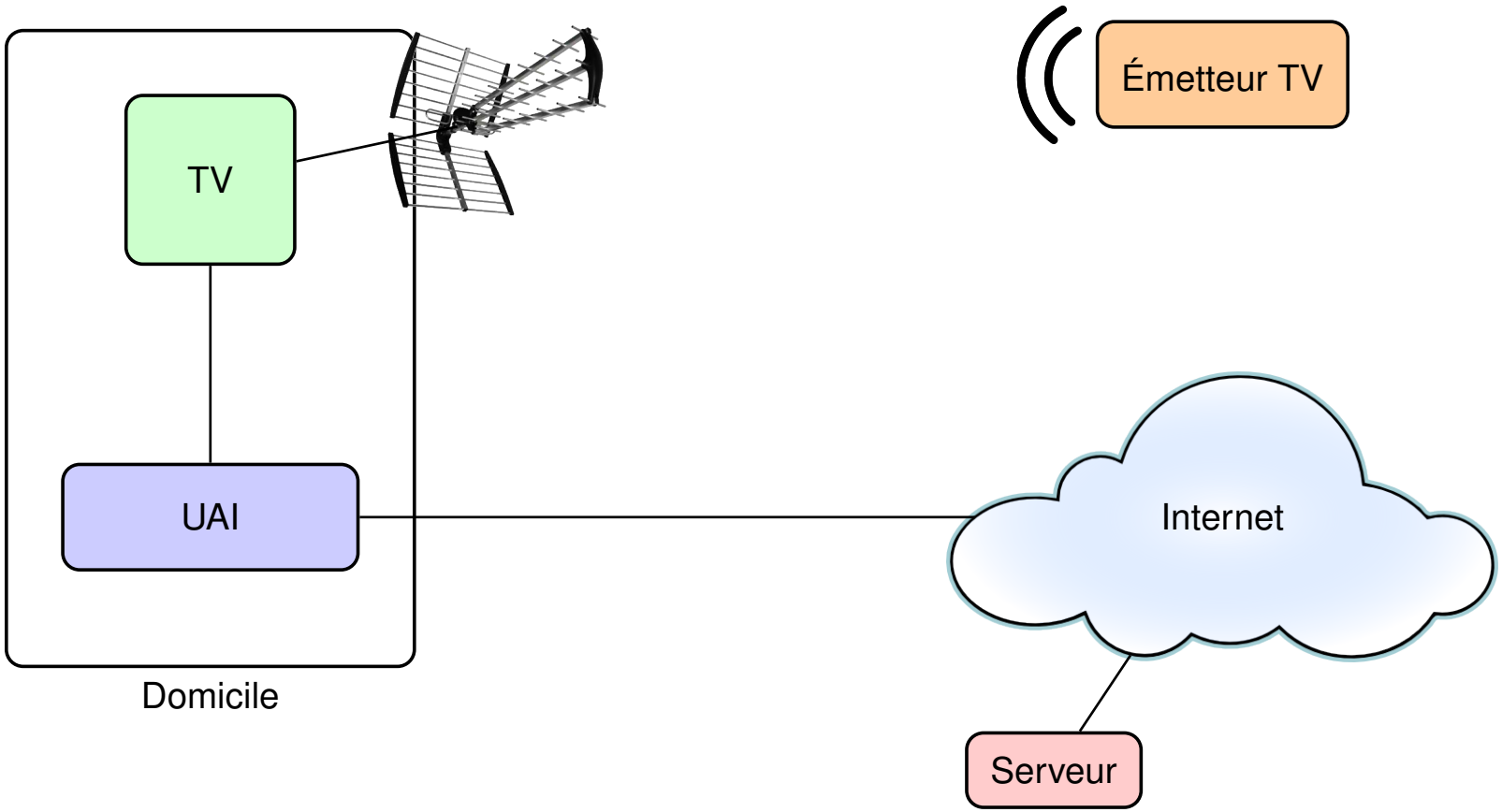
Contenu des flux de données d'un multiplex DVB



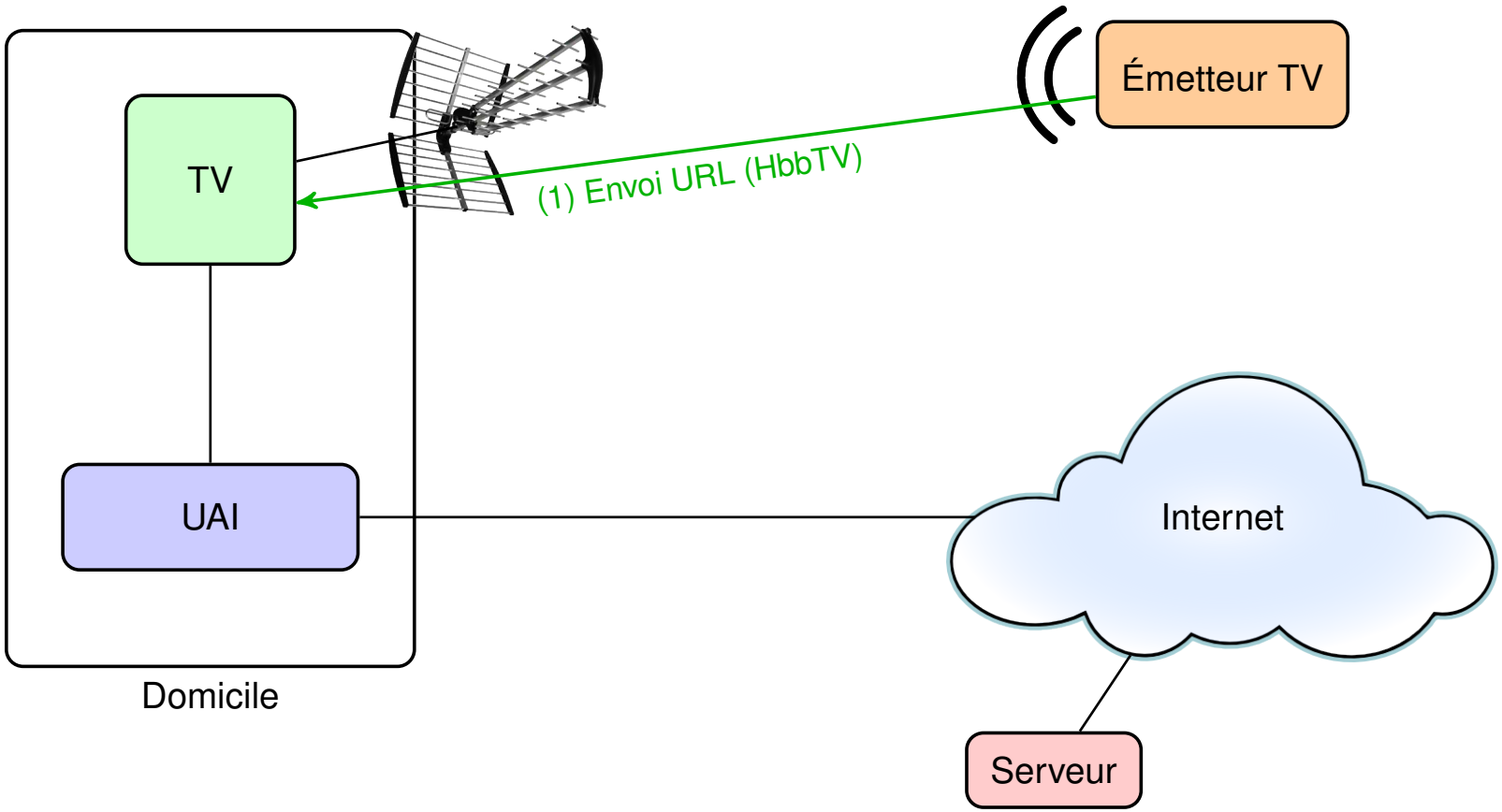
- Informations concernant la chaîne (bouquet, nom, réseau, etc...)
- Informations concernant des "évènements"
- Informations concernant l'heure
- URL du contenu interactif associé à la chaîne TV regardée

Comment fonctionne ce contenu interactif ?

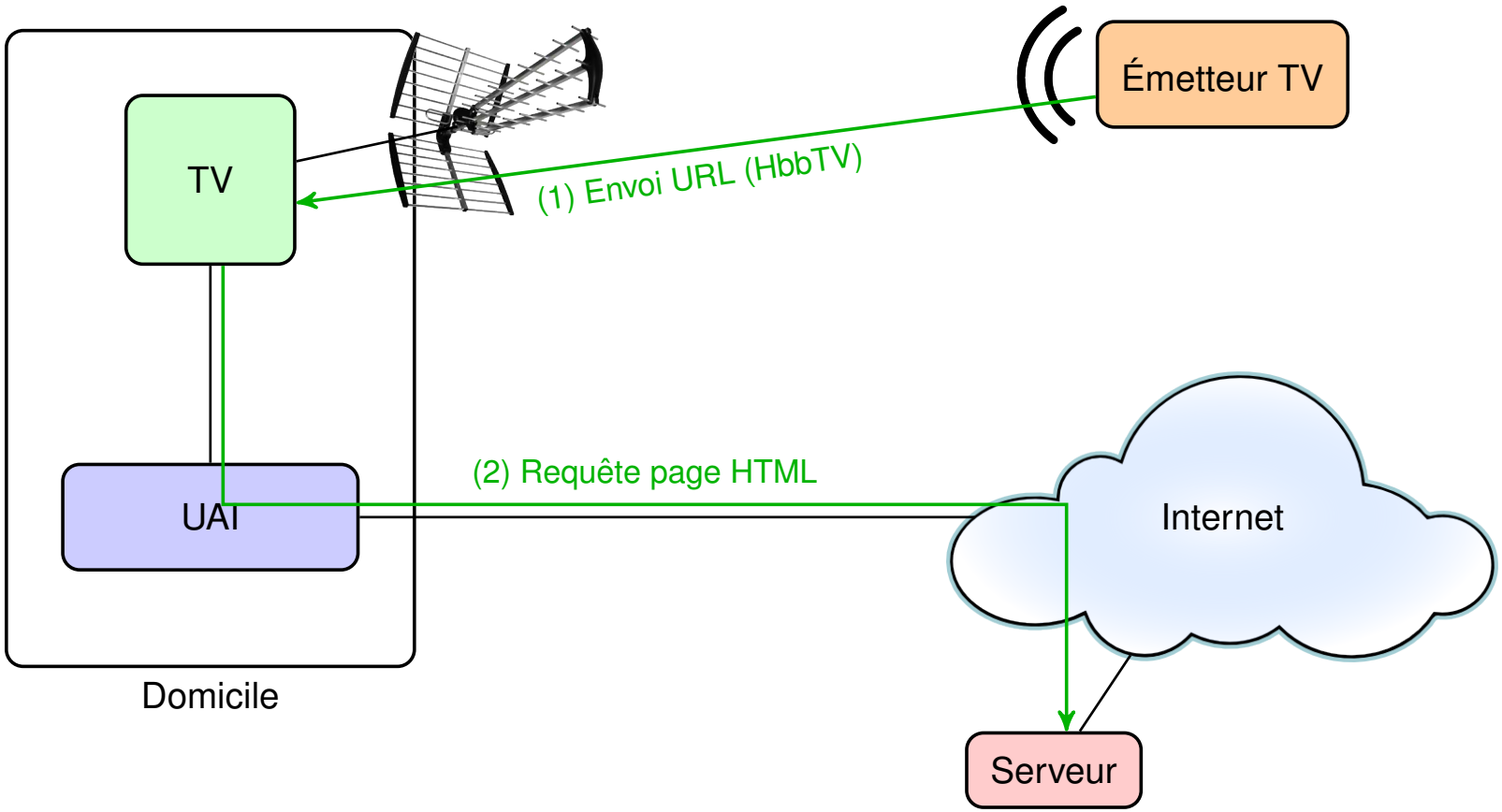
Fonctionnement du contenu interactif



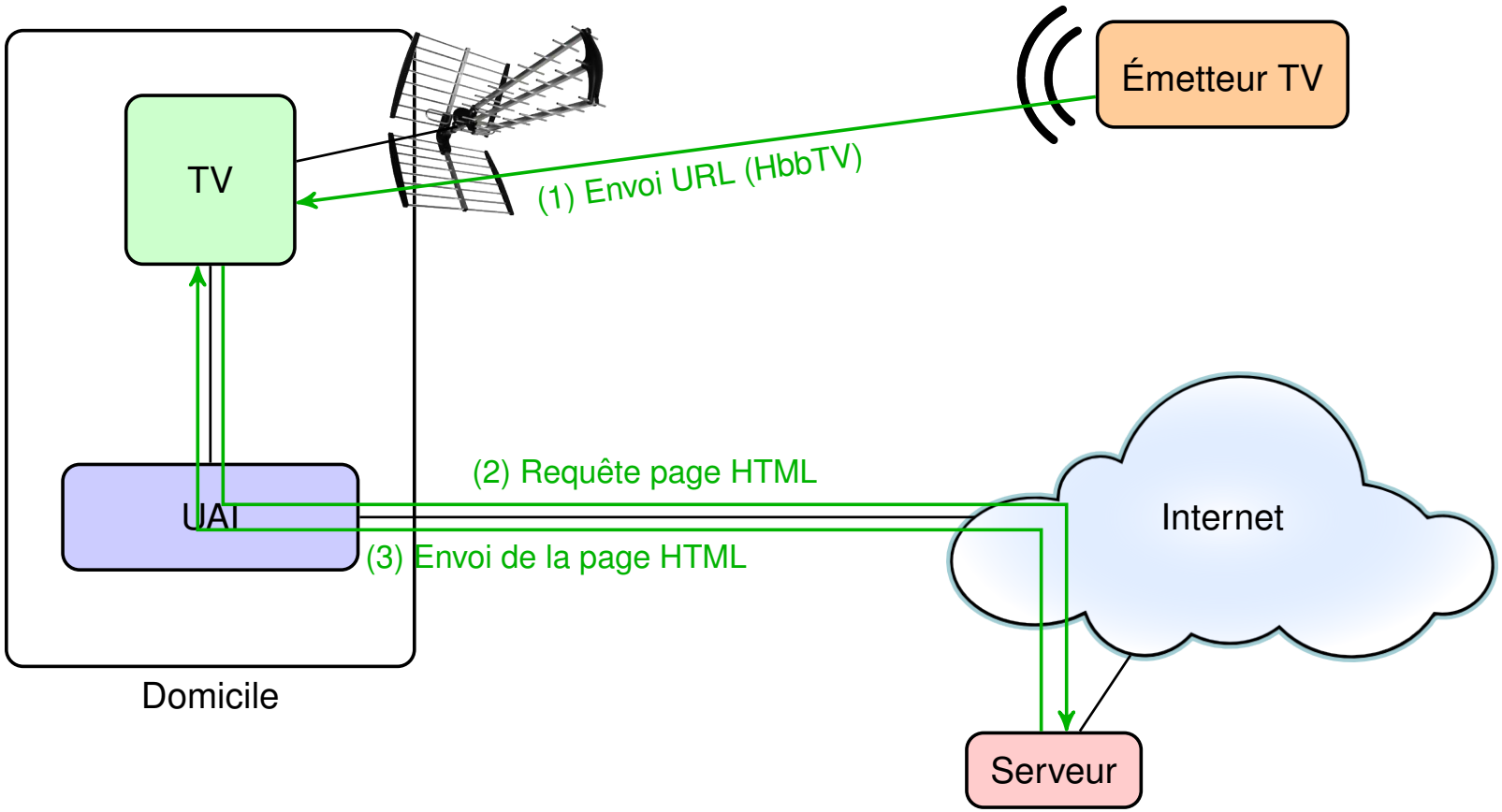
Fonctionnement du contenu interactif



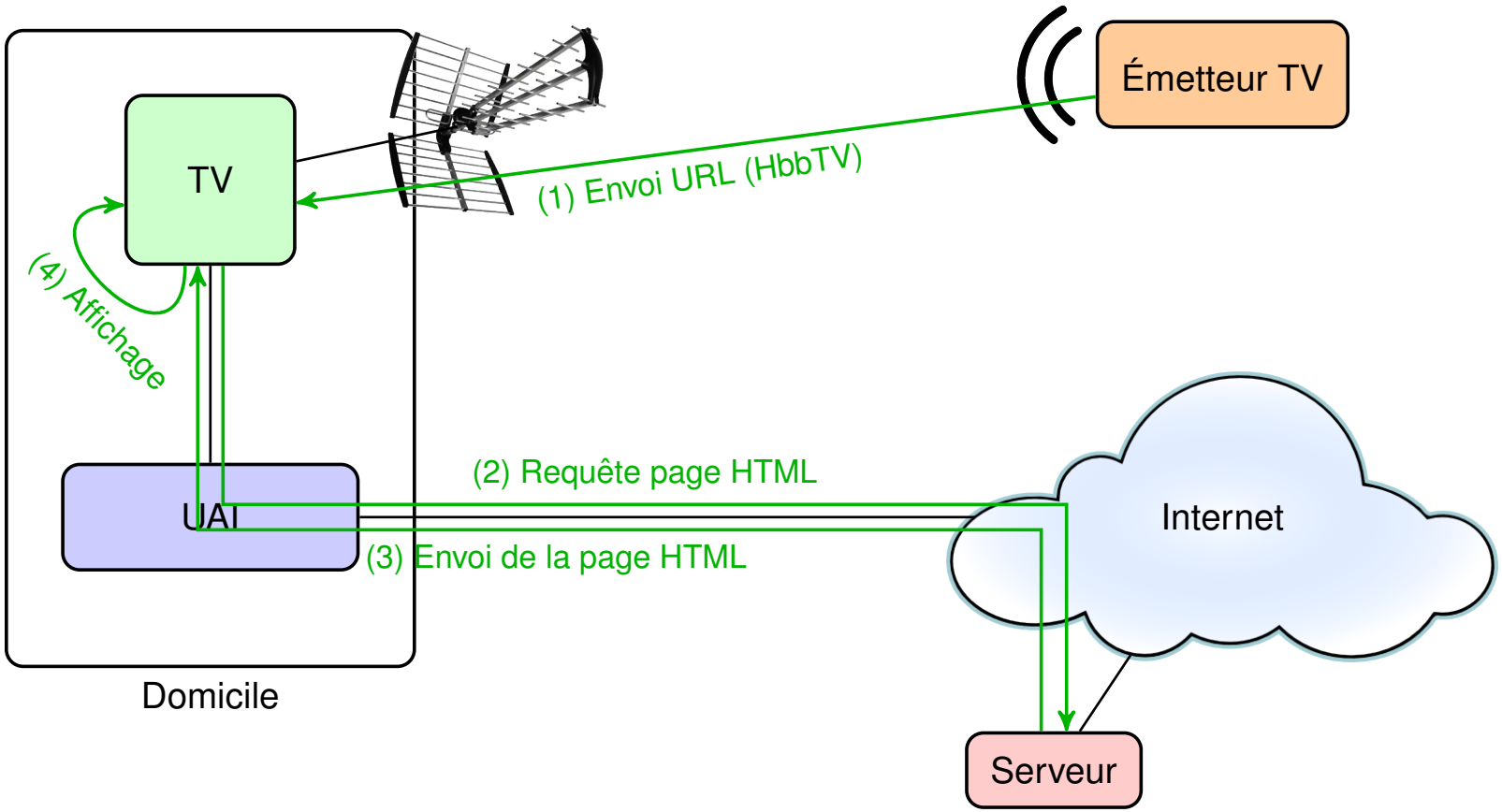
Fonctionnement du contenu interactif



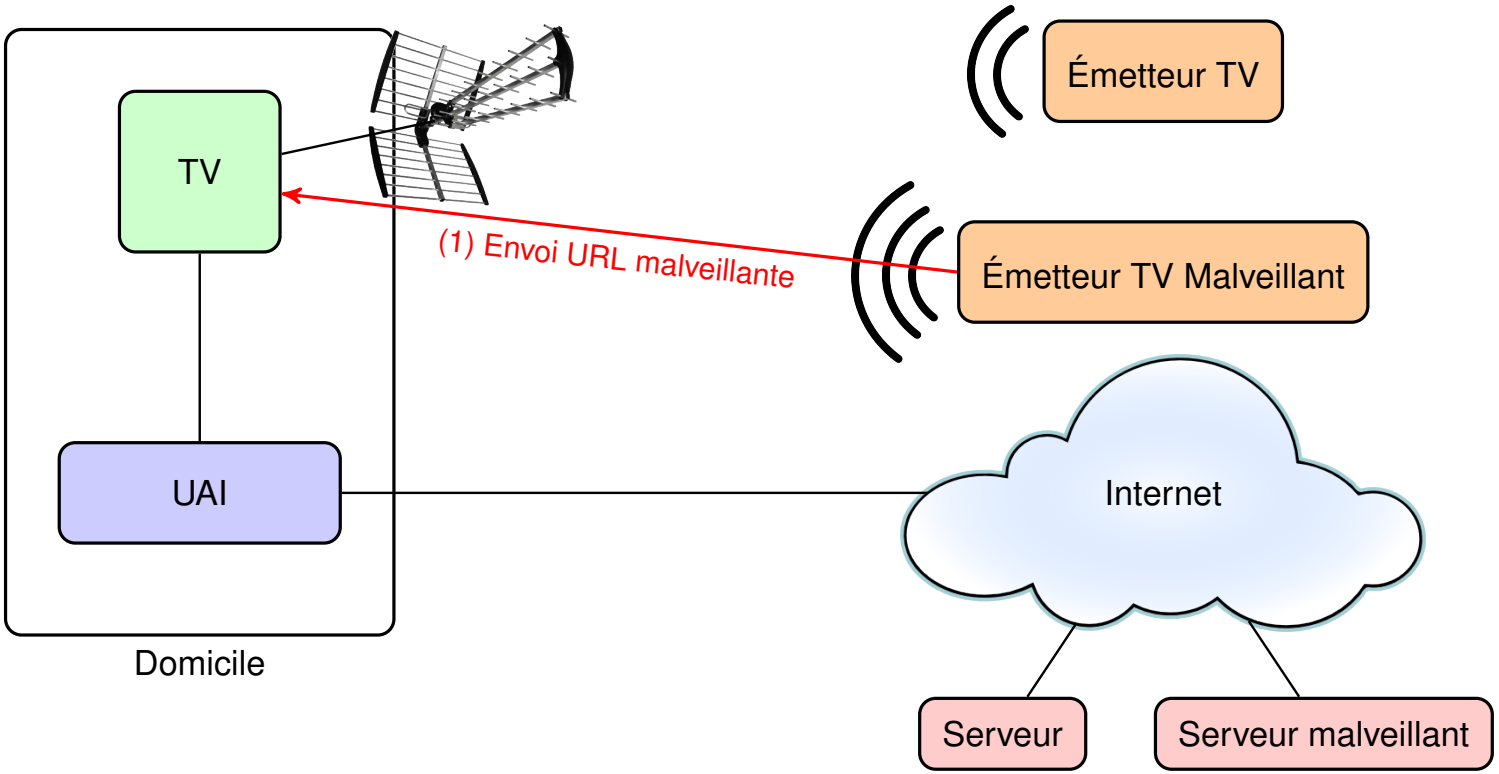
Fonctionnement du contenu interactif



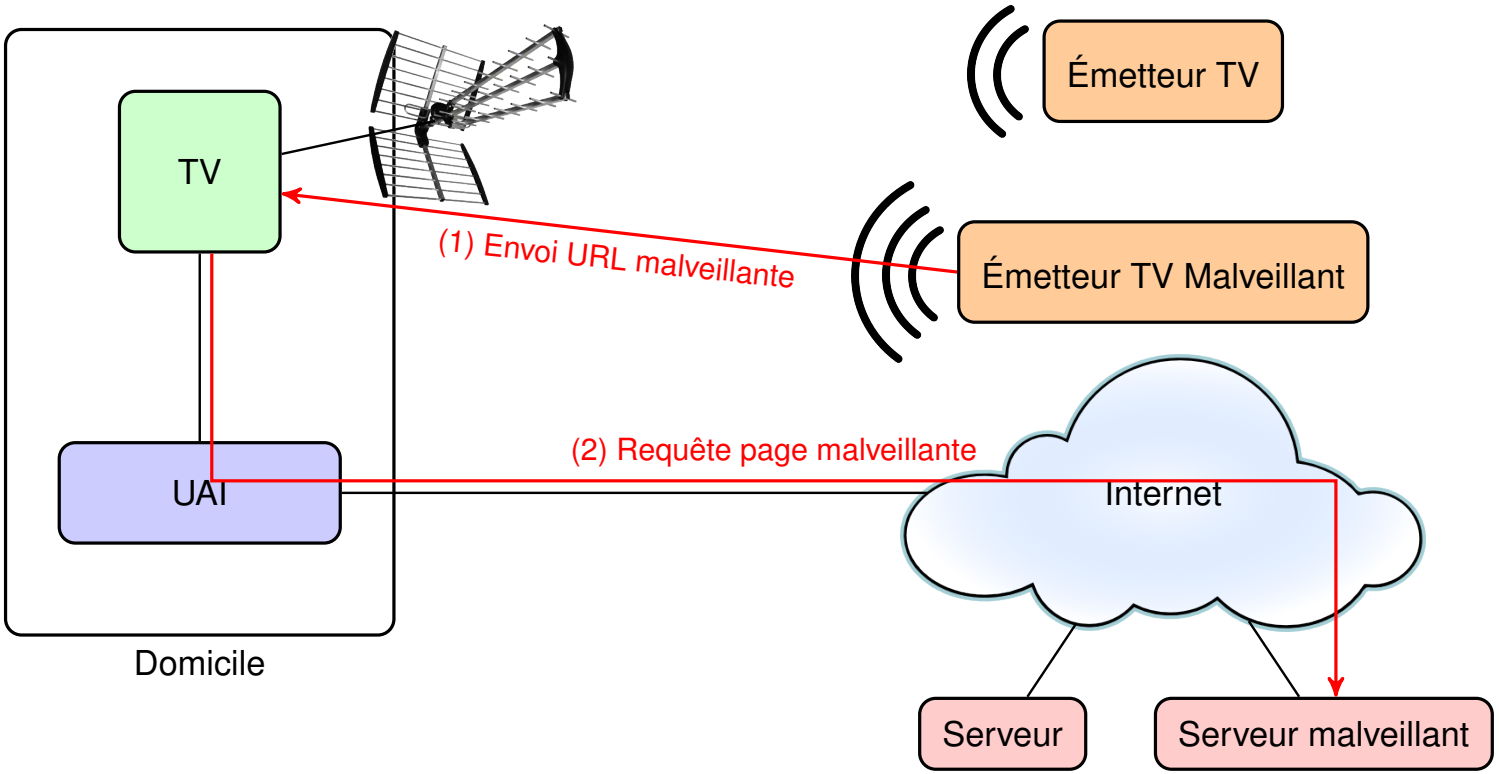
Fonctionnement du contenu interactif



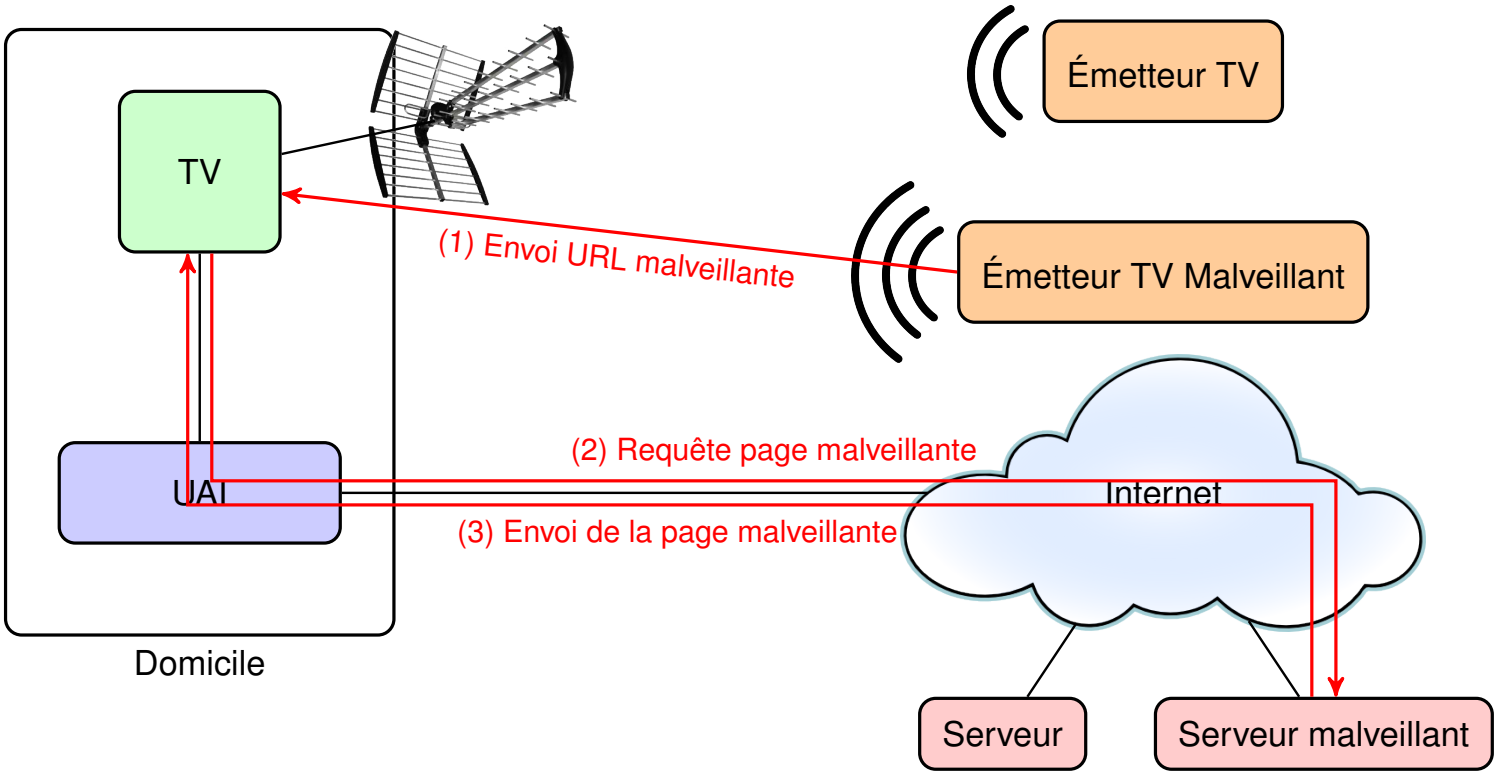
Exemple de contenu interactif malveillant



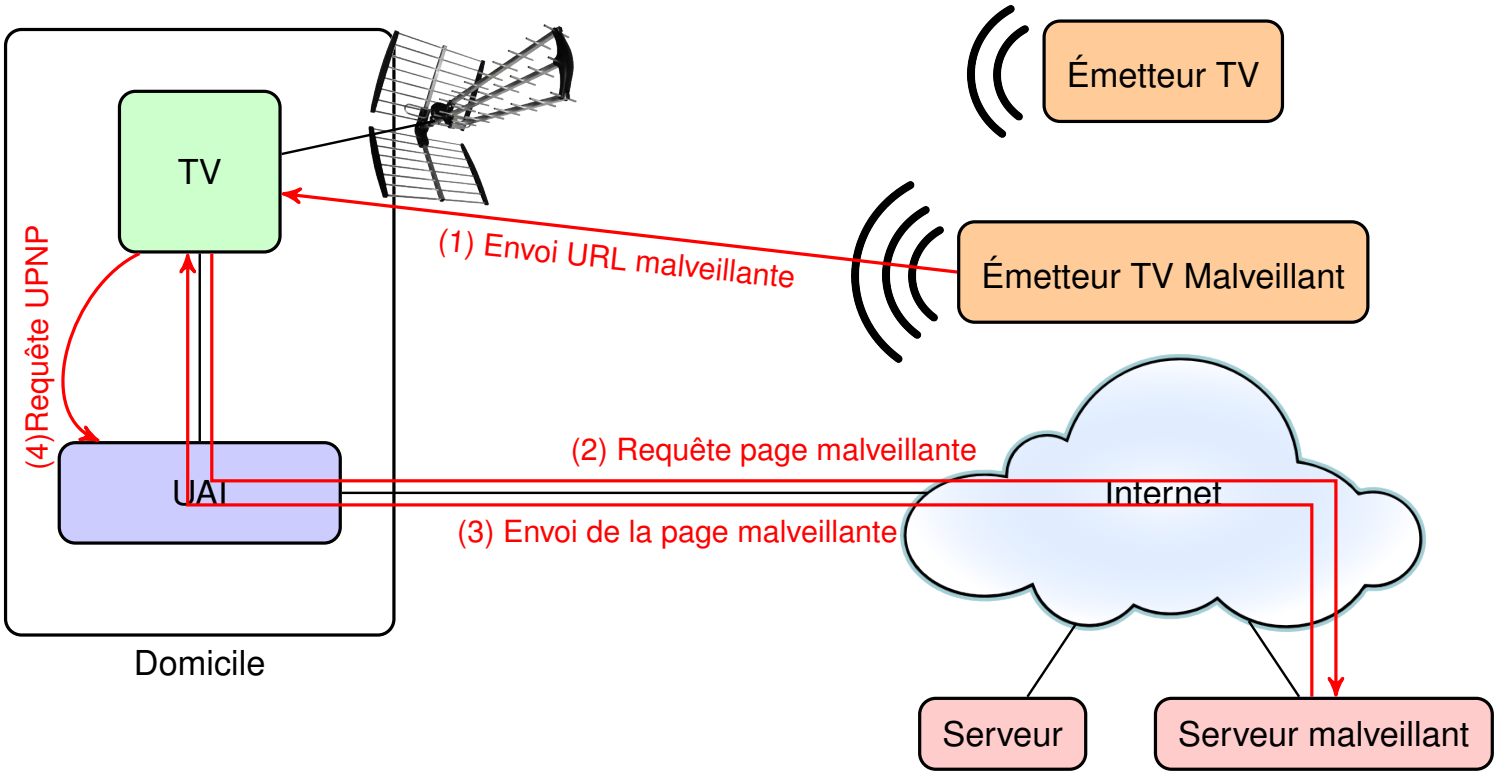
Exemple de contenu interactif malveillant



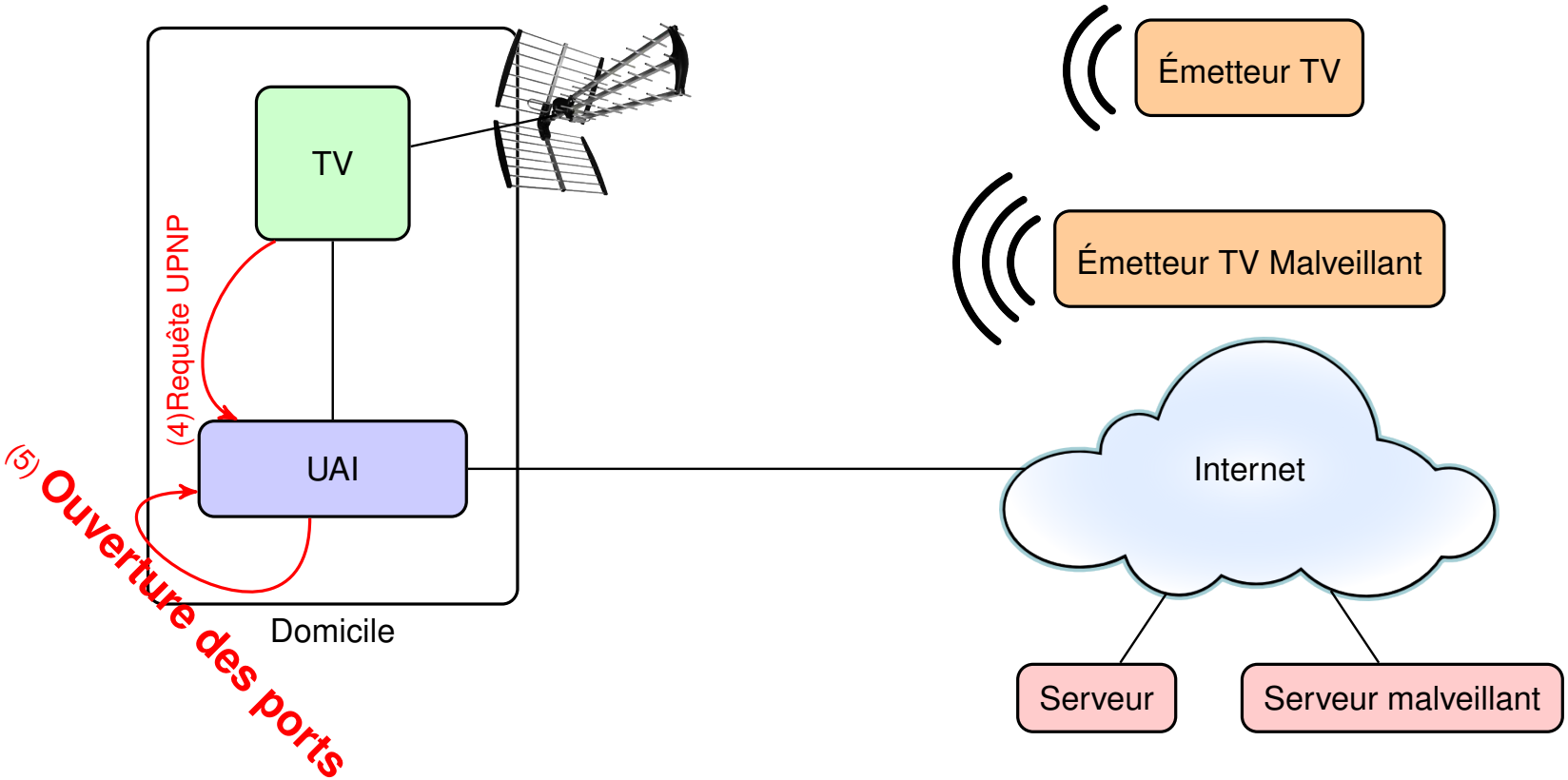
Exemple de contenu interactif malveillant



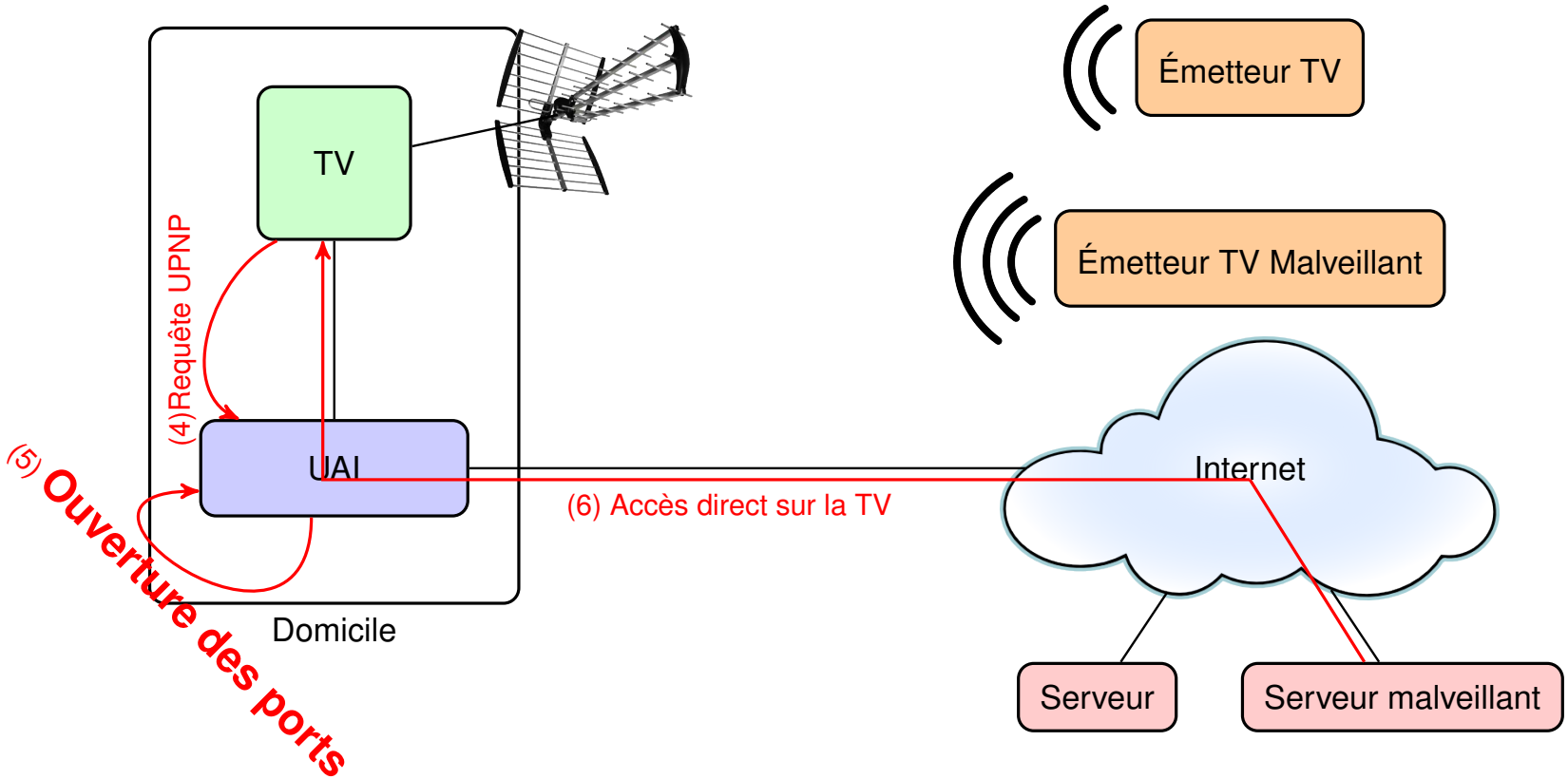
Exemple de contenu interactif malveillant



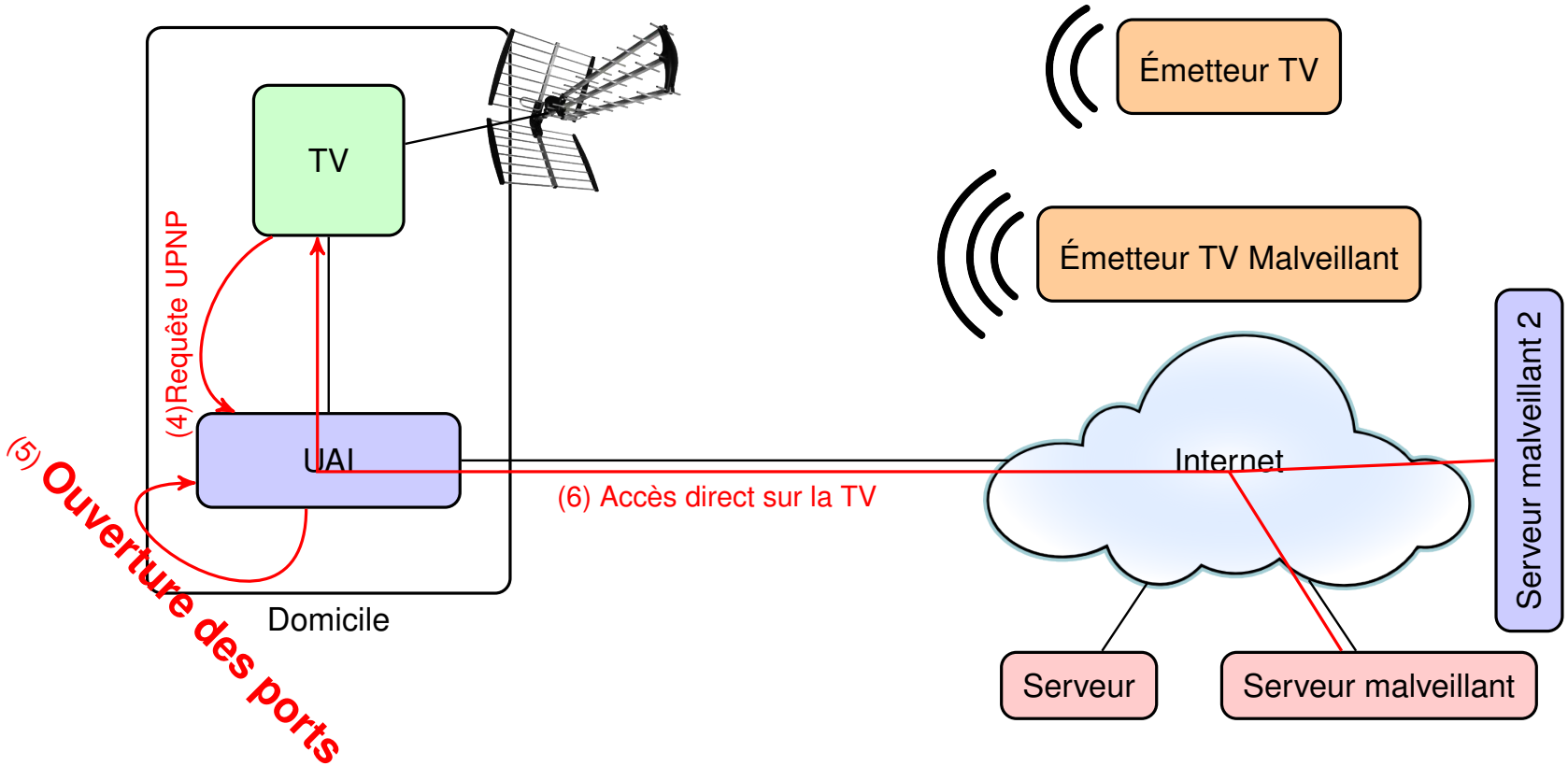
Exemple de contenu interactif malveillant



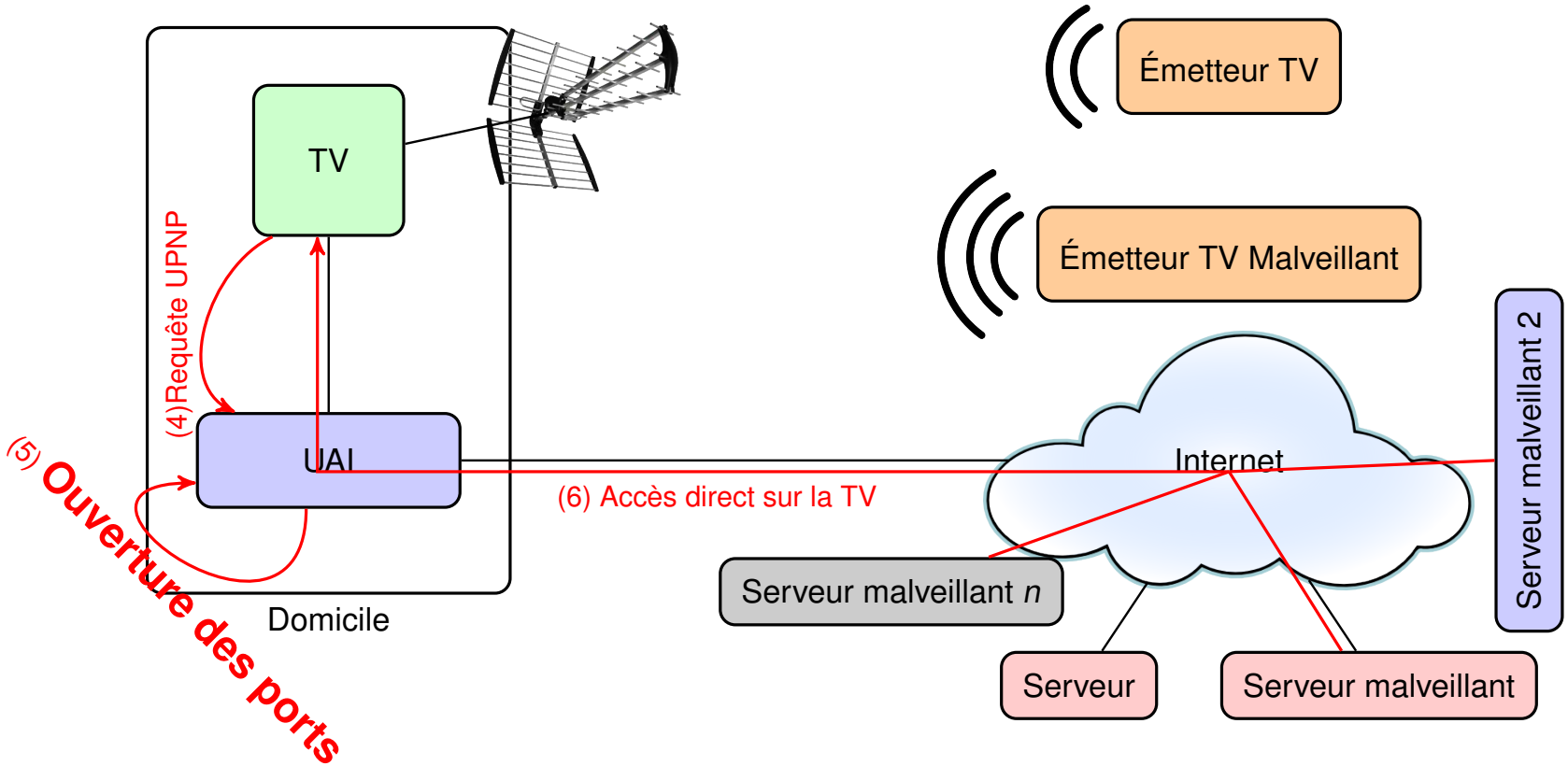
Exemple de contenu interactif malveillant



Exemple de contenu interactif malveillant



Exemple de contenu interactif malveillant



Demo : modification de la configuration de l'UAI ADSL par flux DVB

Travaux concernant le respect de la vie privée

Identification de l'activité de l'utilisateur

- Simulateur de télécommande
- Analyse des données sortantes sur la connexion Internet

→ Des données corrélées à l'activité de l'utilisateur

Utilisation de périphériques de stockage

- Clef USB avec plusieurs fichiers factices
- Analyse des données sortantes sur la connexion Internet

→ Fuite de noms de fichiers

Utilisation et stockage de cookies

- La CNIL impose que le dépositaire de cookies doit en informer l'utilisateur
- L'utilisateur doit pouvoir s'y opposer par l'intermédiaire d'un mécanisme facilement utilisable

→ Des cookies sont déposés par les sites correspondant aux chaînes TV

Travaux concernant le respect de la vie privée

Identification de l'activité de l'utilisateur

- Simulateur de télécommande
- Analyse des données sortantes sur la connexion Internet

→ Des données corrélées à l'activité de l'utilisateur

Utilisation de périphériques de stockage

- Clef USB avec plusieurs fichiers factices
- Analyse des données sortantes sur la connexion Internet

→ Fuite de noms de fichiers

Utilisation et stockage de cookies

- La CNIL impose que le dépositaire de cookies doit en informer l'utilisateur
- L'utilisateur doit pouvoir s'y opposer par l'intermédiaire d'un mécanisme facilement utilisable

→ Des cookies sont déposés par les sites correspondant aux chaînes TV

Travaux concernant le respect de la vie privée

Identification de l'activité de l'utilisateur

- Simulateur de télécommande
- Analyse des données sortantes sur la connexion Internet

→ Des données corrélées à l'activité de l'utilisateur

Utilisation de périphériques de stockage

- Clef USB avec plusieurs fichiers factices
- Analyse des données sortantes sur la connexion Internet

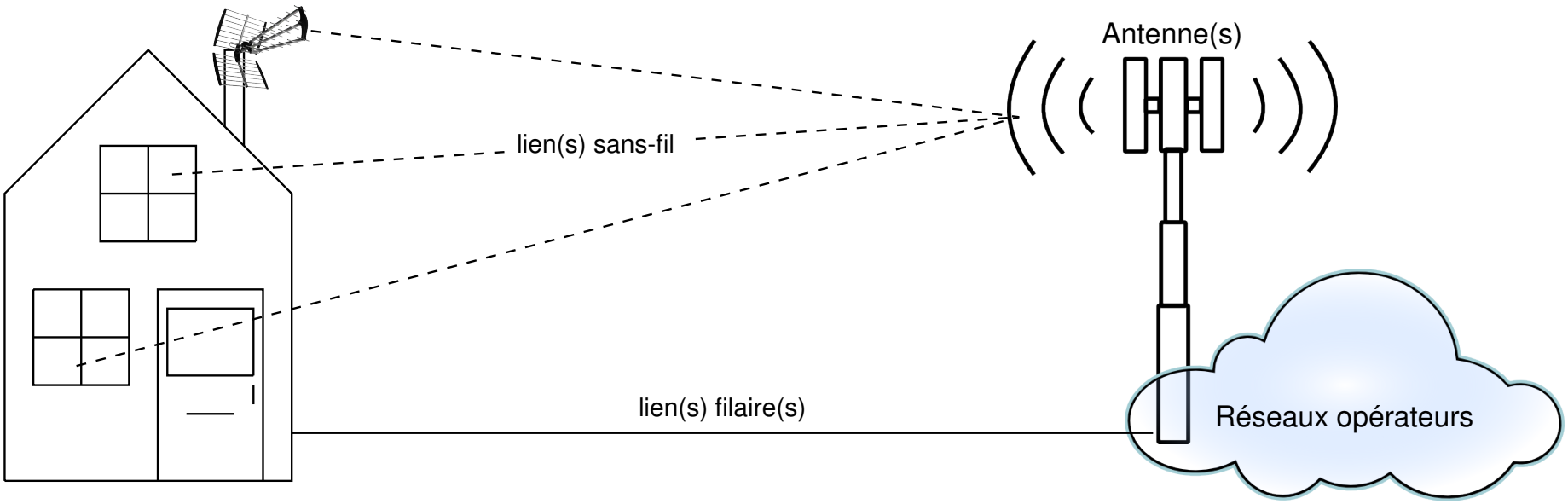
→ Fuite de noms de fichiers

Utilisation et stockage de cookies

- La CNIL impose que le dépositaire de cookies doit en informer l'utilisateur
- L'utilisateur doit pouvoir s'y opposer par l'intermédiaire d'un mécanisme facilement utilisable

→ Des cookies sont déposés par les sites correspondant aux chaînes TV

Résumé



1. Observation sur les liens TV et ADSL
2. Simulation de l'interlocuteur physique : antenne d'émission pour TV et DSLAM pour ADSL
3. Simulation du service fourni : flux DVB et service de mise à jour
4. Étude des données sortantes sur le lien Internet (fuite de données privées)

Plan

Contre-mesures

Que peut-on sécuriser ?

- Identifier la pile de protocole mis en œuvre
- Identifier les mesures pour chaque niveau protocolaire

Que veut-on sécuriser ?

- Étudier le besoin face à chaque critère de sécurité (Disponibilité, Intégrité, Confidentialité et Authenticité)

Choix

- Choisir les différentes mesures capables de répondre aux besoins de sécurité identifiés

Mesures proposées pour la boucle locale (pile IPoPPPoA)

Mécanismes propres à l'application *niveau Application*

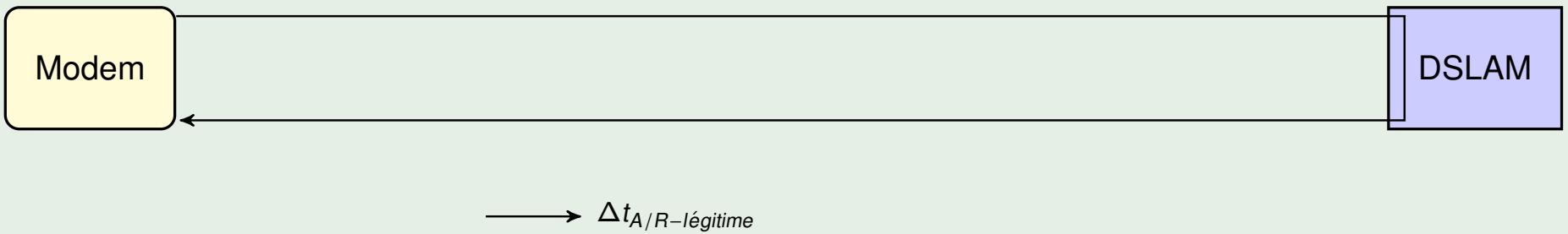
- Utilisation de mécanismes de chiffrement et de signature des données à l'intérieur de l'application
- Nécessite une modification de l'application et une distribution de mise à jour de tous les équipements déjà sur le marché
- Une solution à privilégier dès la conception d'un équipement
- Solution déjà adoptée par bon nombre de téléviseurs

Mesures proposées pour la boucle locale (pile IPoPPPoA)

Mécanismes propres à l'application *niveau Application*

- Utilisation de mécanismes de chiffrement et de signature des données à l'intérieur de l'application
- Nécessite une modification de l'application et une distribution de mise à jour de tous les équipements déjà sur le marché
- Une solution à privilégier dès la conception d'un équipement
- Solution déjà adoptée par bon nombre de téléviseurs

Observation du canal *niveau Physique*

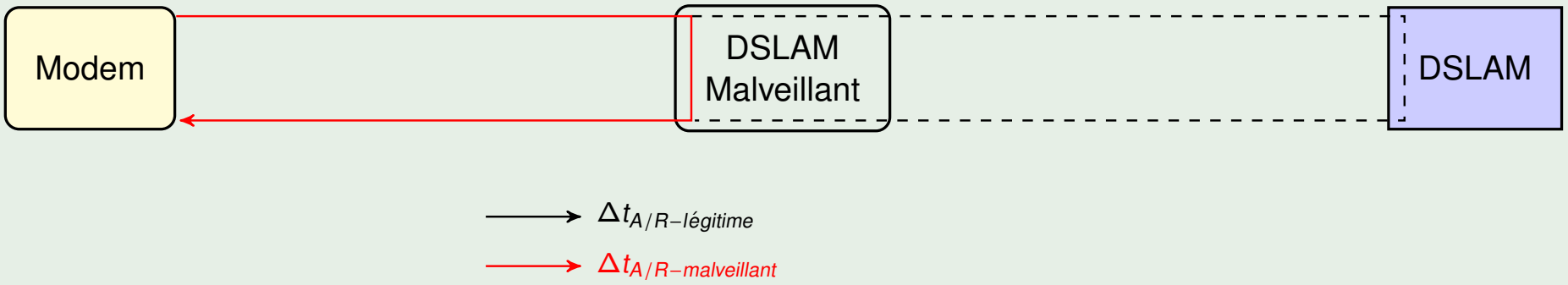


Mesures proposées pour la boucle locale (pile IPoPPPoA)

Mécanismes propres à l'application *niveau Application*

- Utilisation de mécanismes de chiffrement et de signature des données à l'intérieur de l'application
- Nécessite une modification de l'application et une distribution de mise à jour de tous les équipements déjà sur le marché
- Une solution à privilégier dès la conception d'un équipement
- Solution déjà adoptée par bon nombre de téléviseurs

Observation du canal *niveau Physique*



Le flux TV aérien

Pile de protocole utilisée par l'émission DVB-T

№	№ OSI	Nom	Description
3	5-7	Application	Flux élémentaires multimédia & données
2	4	Transport	Multiplexage DVB
1	1-3	Physique	Définition des paramètres de transmission physique

Mesures existantes sur la pile DVB

Digital Rights Management (DRM) *niveau Application*

- DRM est destiné à gérer les droits d'auteur du contenu multimédia d'un flux
- DRM ne fournit aucune sécurité à l'utilisateur

Common Scrambling Algorithm (CSA) *niveau Transport*

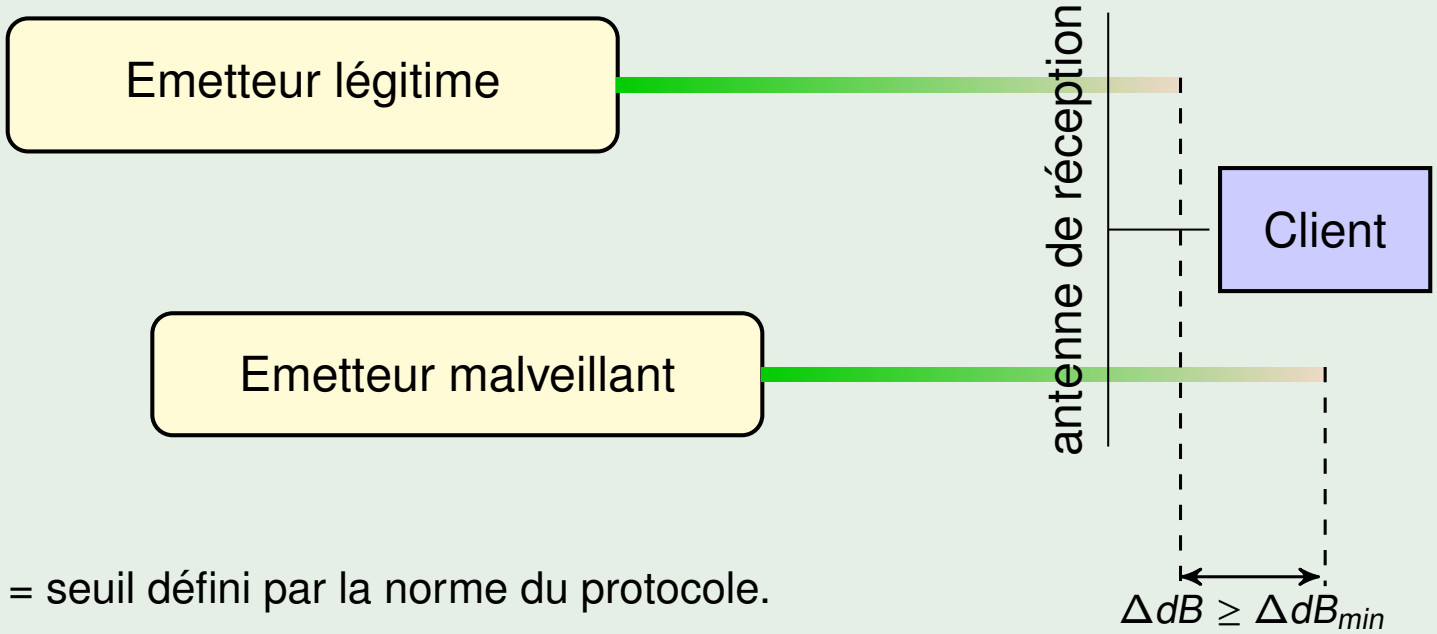
- CSA est destiné à limiter la lecture du contenu du flux aux équipements autorisés (par un abonnement par exemple)
- CSA ne fournit aucune sécurité à l'utilisateur

Mesures proposées sur la pile DVB

Somme de contrôle *niveau Transport*

- Insérer régulièrement une somme de contrôle signée du multiplex DVB
- Permet d'empêcher toute usurpation d'émetteur TV
- Nécessite une bonne gestion (et mise à jour) des clefs utilisées

Observation du canal *niveau Physique*



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

Plan

Conclusion

Sécurité des équipements grand-public connectés

- Une pré-occupation de plus en plus présente
- Rien n'oblige les fabricants à sécuriser leurs équipements
- Un début de prise de conscience par le grand-public

Contributions de cette thèse

- Une méthode d'analyse générique
- Deux cas d'étude concrets
  - Plusieurs problèmes de sécurité identifiés
  - Description de plateformes d'écoute et de simulation sur ADSL et DVB
- Proposition de contre-mesures

Merci


... SINON POUR PROTÉGER VOS
DONNÉES SUR INTERNET,
JE VOUS CONSEILLE CETTE BOX !