Raspberry Spy

Une machine d'interception de paquets à moins de 50$

A. Cervoise

DEVOTEAM
Consulting • Solutions • Expertise

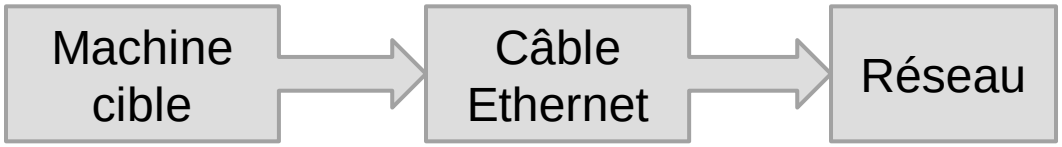
Objectif

- Intercepter les paquets reçus et émis par une machine ou un équipement
  - Pour un audit
  - Pour espionnage (modèle du keylogger)

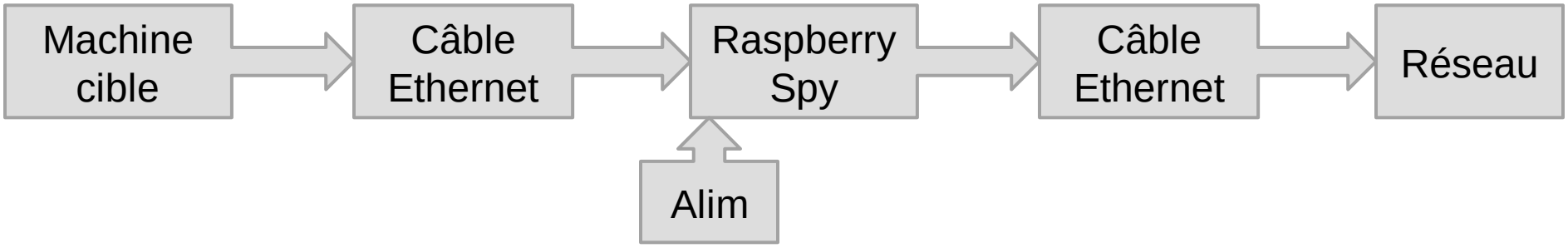
- Un dispositif **portable** et à **bas coup**
  - Moins de 50 $
  - Moins de 2h pour la configuration
  - Pas de connaissance en électronique

Théorie

Sans interception



Avec interception



USB -> Machine cible
USB -> Secteur
USB -> Batterie

Matériel

- Raspberry Pi ~35$
- Carte SD ~5$
- Carte Ethernet en USB ~5$
- Câble USB Mâle A – Micro Mâle B ~2$
- Facultatif :
  - Boitier ~2$
  - Patin collant

Logiciel

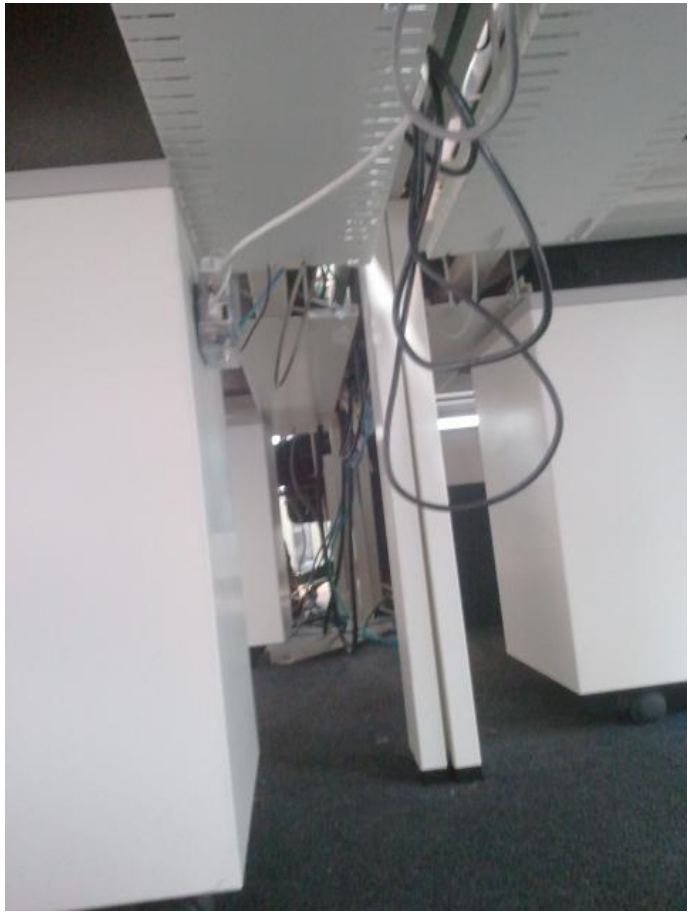
- Raspbian
  - Basée sur Debian
- Quelques paquets
  - bridge-utils
    - le raspberry spy se comporte comme un bridge
  - tcpdump
    - capture les paquets au démarrage

Logiciel

- Exploitation des captures
  - Wireshark
    - Analyseur de paquets
  - dsniff
    - Utilitaire d'audit réseau permettant de sniffer les mots de passe circulants en clair dans des protocoles non sécurisés
  - Xplico
    - Outil d'analyse forensic de captures réseau

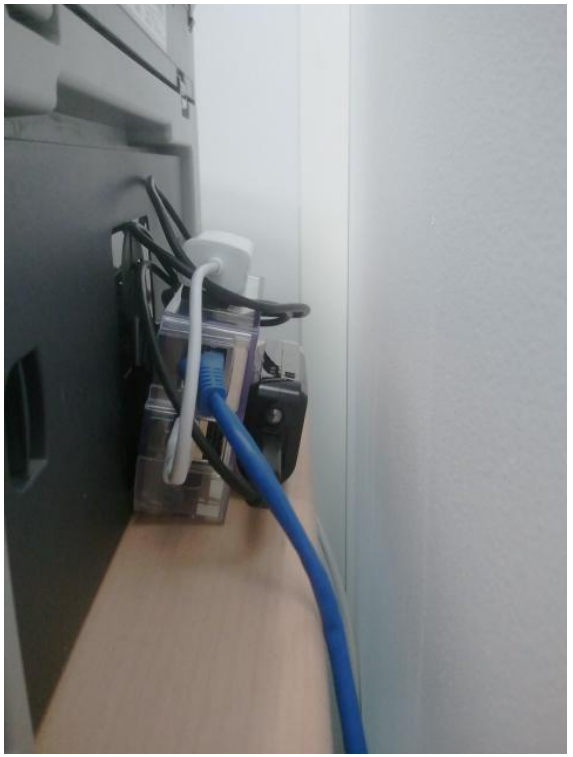
Exemples d’utilisation

- Bureau



Exemples d’utilisation

- Imprimante



Limites matériels

- Alimentation en USB
  - Utiliser une prise secteur
  - Emprunter une prise à la machine cible
    - Simple sur une imprimante
- Ne supporte pas la PoE
  - Impossible de capturer des paquets sur un équipement alimenté en PoE

Limites logiciels

- Raspian inclus de nombreux paquets inutiles dans notre cas
- Le comportement du dispositif n'est pas défini lorsque le disque est plein
- La récupération des paquets n'est pas automatique sous Windows

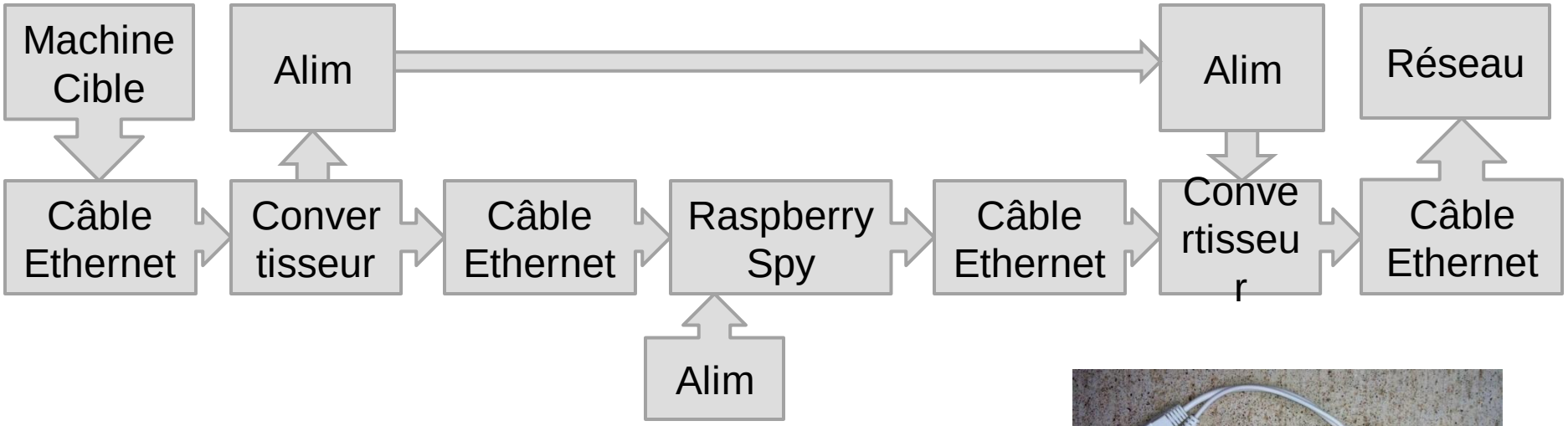
Evolution

- Facultatif :
  - Alimentation externe ~3$
    - Durée de capture : environ 3h avec deux piles AA.

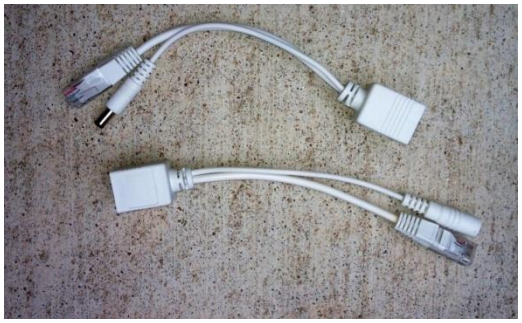
Améliorations envisageables

- Transférer les informations sur une machine distante (réseau local, internet, fax, etc.)
- Utiliser une véritable batterie (~100$)
- Mettre en place un dispositif de transfert de la PoE

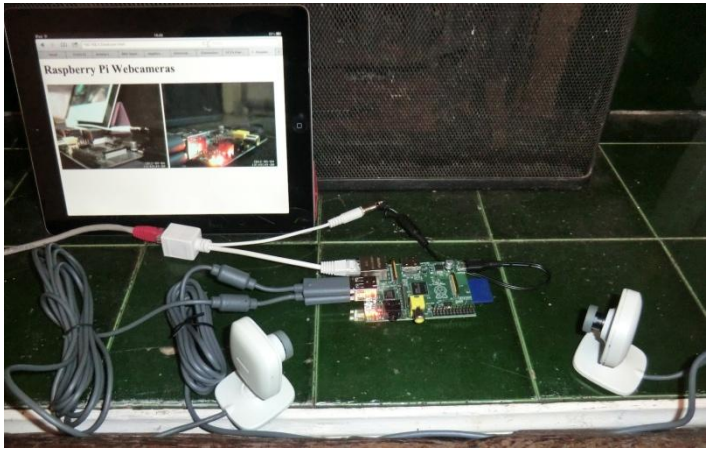
Transfert de la PoE

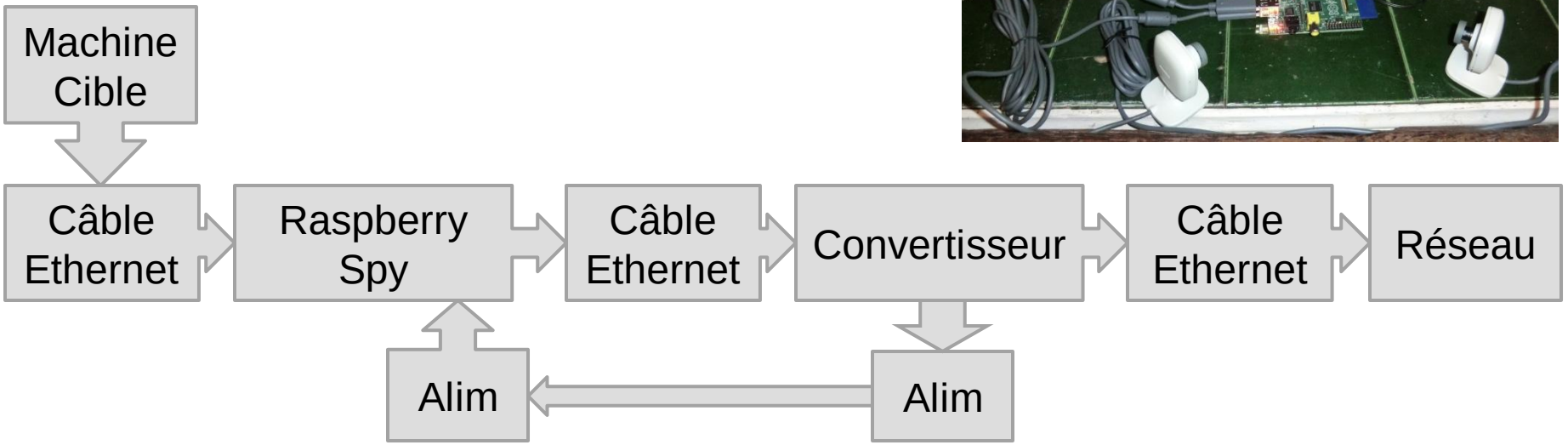


USB -> Machine cible
USB -> Secteur
USB -> Batterie



Utilisation de la PoE





Source image :
http://astrobeano.blogspot.fr/2012/08/power-over-ethernet-for-raspberry-pi.html